

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 1 4 4 6 7
Application Number:

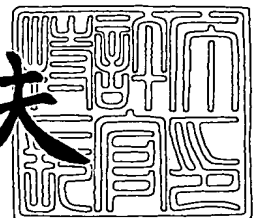
[ST. 10/C] : [J P 2 0 0 3 - 3 1 4 4 6 7]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫





【書類名】 特許願
【整理番号】 0304619
【提出日】 平成15年 9月 5日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 12/00
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 金井 洋一
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 斉藤 敦久
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 谷内田 益義
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-269102
 【出願日】 平成14年 9月13日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-299712
 【出願日】 平成14年10月11日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

ドキュメントファイルに関連付けられている印刷要件を取得する手段と、
上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを
備えたことを特徴とするドキュメント印刷プログラム。

【請求項 2】

暗号化された上記ドキュメントファイルの復号時に上記印刷要件を伴った印刷処理を実
行することで上記印刷要件の強制を行う請求項 1 に記載のドキュメント印刷プログラム。

【請求項 3】

暗号化された上記ドキュメントファイルの復号鍵を取得する手段と、
取得した復号鍵に基づいて上記ドキュメントファイルを復号する手段と、
上記ドキュメントファイルに関連付けられている上記印刷要件を取得する手段と、
取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えた請求項 2 に記載の
ドキュメント印刷プログラム。

【請求項 4】

復号された上記ドキュメントファイルから上記印刷要件を取得する請求項 3 に記載のド
キュメント印刷プログラム。

【請求項 5】

上記ドキュメントファイルを暗号化した暗号鍵に対応するパスワードを入力して復号鍵
を生成する請求項 4 に記載のドキュメント印刷プログラム。

【請求項 6】

内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項 5 に記載
のドキュメント印刷プログラム。

【請求項 7】

上記ドキュメントファイルに関連付けられた上記印刷要件をネットワークを介してサー
バから取得する請求項 3 に記載のドキュメント印刷プログラム。

【請求項 8】

上記サーバに対してユーザの認証を行う手段と、
認証した上記ユーザの印刷要件を上記ドキュメントファイルに関連付けられて上記サー
バに登録されたユーザ毎の印刷要件を含む ACL から取得する手段とを備えた請求項 7 に
記載のドキュメント印刷プログラム。

【請求項 9】

上記ドキュメントファイルを暗号化した暗号鍵に相当するパラメータをネットワークを
介してサーバから取得し、このパラメータから復号鍵を導出する請求項 8 に記載のドキュ
メント印刷プログラム。

【請求項 10】

内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項 9 に記載
のドキュメント印刷プログラム。

【請求項 11】

上記ドキュメントファイルに含まれるパラメータを上記復号鍵の生成に利用する請求項
9 または 10 のいずれか一項に記載のドキュメント印刷プログラム。

【請求項 12】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、
指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、
上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えたことを特徴とする
ドキュメント保護プログラム。

【請求項 13】

上記ドキュメントファイルに上記印刷要件を付与してから暗号化することにより上記ド
キュメントファイルと上記印刷要件とを関連付ける請求項 12 に記載のドキュメント保護
プログラム。

【請求項 14】

入力されたパスワードに基づいて暗号鍵を生成する請求項 13 に記載のドキュメント保護プログラム。

【請求項 15】

内部で保持もしくは生成したパラメータを上記暗号鍵の生成に利用する請求項 14 に記載のドキュメント保護プログラム。

【請求項 16】

上記ドキュメントファイルに関連付けられた上記印刷要件をネットワークを介してサーバに登録する請求項 12 に記載のドキュメント保護プログラム。

【請求項 17】

上記印刷要件を上記ドキュメントファイルに関連付けた ACL の一部として登録する請求項 16 に記載のドキュメント保護プログラム。

【請求項 18】

暗号化に用いた暗号鍵を上記サーバに登録する請求項 17 に記載のドキュメント保護プログラム。

【請求項 19】

暗号化に用いた暗号鍵の導出に用いたパラメータを上記サーバに登録する請求項 18 に記載のドキュメント保護プログラム。

【請求項 20】

暗号化に用いた暗号鍵の導出に用いたパラメータを上記ドキュメントファイルの一部に付与する請求項 18 または 19 のいずれか一項に記載のドキュメント保護プログラム。

【請求項 21】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、

暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。

【請求項 22】

ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、

暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。

【書類名】明細書

【発明の名称】ドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システム

【技術分野】**【0001】**

本発明はドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムに関する。

【背景技術】**【0002】**

近年、文書や画像などの情報（以下、ドキュメントという）を取り扱うオフィスなどにおいては、ドキュメントを紙に印刷する代わりにドキュメントファイルとして情報記録媒体へ電子的に記録しておく手法が主流となっている。

【0003】

ドキュメントを電子的に記録すれば、紙資源を用いることなくドキュメントを記録できるため、省資源化を図れるとともに、ドキュメントが印刷された紙を格納する必要がなくなり、省スペース化を実現できる。

【0004】

また、ドキュメントを電子的に記録すれば、同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布したりすることが可能となり、業務の効率化を図ることができる。

【0005】

同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布できるというドキュメントを電子的に記録する場合の長所は、ドキュメントが漏洩しやすくなるという問題の裏返しでもある。

【0006】

オフィスなどにおいて取り扱われるドキュメントの中には、機密性を要するものも多数存在するため、ドキュメントの漏洩を防止するための対策を講じる必要がある。

【0007】

ドキュメントの漏洩を防止することを目的とした従来技術としては、特許文献1に開示される「Method of encrypting information for remote access while maintaining access control」、特許文献2に開示される「Information security architecture for encrypting documents for remote access while maintaining access control」、および、特許文献3に開示される「文書管理システム」のように、ドキュメントファイルを開く際にユーザ認証を求めて、正当なユーザだけがドキュメントの内容を参照できるようにする手法や、開いたドキュメントファイルを印刷しようとする際にユーザに印刷する権限があるか否かをチェックして権限があるユーザにのみ印刷させるものがある。

【0008】

また、特許文献4に開示される「電子的に伝送された情報の印刷制限方法および印刷制限付き文書」のように、支払いを済ませた場合にのみ印刷が許可されるようにドキュメントファイルをコントロールするような技術もある。

【特許文献1】 米国特許第6339825号明細書

【特許文献2】 米国特許第6289450号明細書

【特許文献3】 特開2001-142874号公報

【特許文献4】 特開2002-024097号公報

【発明の開示】**【発明が解決しようとする課題】****【0009】**

上記各特許文献に開示される発明においては、権限のない者がドキュメントを印刷できないように設定できるものの、印刷した物（プリントアウト）に対するセキュリティは何ら設定されていない。

【0010】

よって、印刷する権限を有するユーザになりすまして一度ドキュメントを印刷してしまえば、その後は何の制約を受けることなくドキュメントのプリントアウトを複製して他者に配布できることになる。

【0011】

さらに、ドキュメントを漏洩させようとする者が印刷する権限を有する正当なユーザである場合は、これを阻止することはできない。

【0012】

このように、従来の技術では、ドキュメントファイルの使い勝手が良くないとともに、プリントアウトによるドキュメントの漏洩を防止するためのセキュリティが不十分であるという問題があった。

【0013】

本発明はかかる問題に鑑みてなされたものであり、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。

【課題を解決するための手段】**【0014】**

上記の目的を達成するため、本発明のドキュメント印刷プログラムは、ドキュメントファイルに関連付けられている印刷要件を取得する手段と、上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを備えるようにしている。

【0015】

これにより、印刷時におけるセキュリティ対策を強制することができる。

【0016】

また、暗号化された上記ドキュメントファイルの復号時に上記印刷要件を伴った印刷処理を実行することで上記印刷要件の強制を行うようにすることができる。

【0017】

これにより、暗号化技術を用いた堅牢なシステムが構築できる。

【0018】

また、暗号化された上記ドキュメントファイルの復号鍵を取得する手段と、取得した復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている上記印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えるものとして構成できる。

【0019】

また、本発明のドキュメント保護プログラムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えるものとして構成できる。

【0020】

また、本発明のドキュメント保護システムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとして構成できる。

【0021】

また、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、暗

号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとしても構成できる。

【発明の効果】

【0022】

本発明によれば、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供できる。

【発明を実施するための最良の形態】

【0023】

〔第1の実施形態〕

本発明を好適に実施した第1の実施形態について説明する。

【0024】

図1に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【0025】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末101とユーザ端末102とプリンタ103とを有する。配布者端末101およびユーザ端末102は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末101にはドキュメント保護プログラム111が、ユーザ端末102にはドキュメント印刷プログラム121がそれぞれ実装されている。

【0026】

ドキュメント保護プログラム111は、ドキュメントファイルに配布者端末101の使用者（以下、配布者という）の入力操作に応じて印刷要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。図2はドキュメント保護プログラム111の構成例を示したものであり、属性付与部111aと暗号化部111bと暗号鍵取得部111cとパラメータ取得部111dとを含んでいる。なお、パラメータ取得部111dは任意的要素である。各部の機能については後の動作において説明する。

【0027】

図1に戻り、ドキュメント印刷プログラム121は、ユーザ端末102の使用者（以下、ユーザという）の入力操作に応じ、保護ドキュメントを復号するとともに設定されている印刷要件に応じた印刷処理をプリンタ103に実行させる処理を行うプログラムである。図3はドキュメント印刷プログラム121の構成例を示したものであり、復号部121aと復号鍵取得部121bとパラメータ取得部121cと印刷要件取得部121dと印刷処理部121eとを含んでいる。なお、パラメータ取得部121cは任意的要素である。また、図4は図3における印刷処理部121eの構成例を示したものであり、要件処理部121fとドキュメント加工部121gとプリンタドライバ121hと警告表示部121iとログ記録部121jとを含んでいる。各部の機能については後の動作において説明する。

【0028】

なお、配布者の入力操作に応じてドキュメント保護プログラム111がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、BDPという）、機密印刷（Private Access：以下、PACという）、電子透かし（Digital Watermark：以下、DWMという）の付加、バーコード付加（Embedding Barcode：以下、EBCという）、機密ラベルスタンプ（Security Label Stamp：以下、SLSという）などが挙げられる。

【0029】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。まず、システム全体の動作について説明する。

【0030】

図1において、配布者は、配布者端末101を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0031】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末101の入力装置を操作してドキュメントファイルをドキュメント保護プログラム111に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム111は、暗号化に用いられドキュメントファイルにアクセスするために必要となるパスワードと、印刷時に強制したいセキュリティ処理（すなわち、印刷要件）との設定を配布者に要求する。例えば、ドキュメント保護プログラム111は、配布者端末101の表示装置にメッセージを表示するなどして、パスワードと印刷要件の設定を要求する。図5はパスワードと印刷要件の設定を要求する画面の例を示したものであり、必要事項を入力したりチェックボックスから選択が行えるようになっている。なお、図5の画面では保護するドキュメントファイルを指定することもできるようになっている。

【0032】

配布者が配布者端末101の入力装置を介してパスワードおよび印刷要件を入力すると、ドキュメント保護プログラム111はこれを取得する。なお、ドキュメント保護プログラム111はその後に生成する保護ドキュメントの保存場所を問い合わせるため、例えば図6に示すような画面を表示装置に表示する。

【0033】

ドキュメント保護プログラム111は、取得したパスワードと印刷要件とを用いてドキュメントファイルから保護ドキュメントを生成する。

【0034】

配布者は、ドキュメント保護プログラム111が生成した保護ドキュメントをユーザに受け渡すとともに、ドキュメントファイルにアクセスするために必要となるパスワードをユーザに通知する。

【0035】

ユーザがドキュメントファイルを印刷しようとする場合には、ユーザ端末102に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末102が配布者端末101と通信可能である場合には、通信網を介して配布者端末101から保護ドキュメントを取得するようにしてもよい。

【0036】

ユーザが、ユーザ端末102の入力装置を介してドキュメント印刷プログラム121に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム121は、ドキュメントファイルにアクセスするために必要となるパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム121は、ユーザ端末102の表示装置にメッセージを表示するなどして、パスワードの入力を要求する。図7はパスワードを要求する画面の例を示したものであり、印刷しようとしたドキュメントファイルが保護されている旨の説明文が伴われている。

【0037】

ユーザが、配布者から通知されたパスワードを入力装置を介してユーザ端末102へ入力すると、ドキュメント印刷プログラム121は、入力されたパスワードを用いて保護ドキュメントをドキュメントファイルに復元し、設定されている印刷要件を満たすようにプリンタ103に印刷処理を実行させる。例えば、ドキュメントファイルに前述したBDP

が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0038】

これにより、ドキュメントを印刷する際に、配布者が設定した印刷要件を強制することが可能となる。

【0039】

なお、ユーザが印刷要件について意識していない場合があると共に、印刷要件によっては特定のプリンタでないと処理できないものもあるため、印刷の実行前にその旨の情報がユーザに提供されることが望ましい。図8はユーザ端末102の表示装置上に表示される確認画面の例を示したものであり、印刷要件と利用できるプリンタとが表示され、使用するプリンタを選択することができるようになっている。

【0040】

次に、ドキュメント保護プログラム111の動作（保護ドキュメントを生成する処理）およびドキュメント印刷プログラム121の動作（保護ドキュメントを印刷する処理）についてさらに詳しく説明する。

【0041】

図9に、ドキュメント保護プログラム111の動作を示す。

【0042】

まず、ドキュメント保護プログラム111は、配布者が配布者端末101の入力装置を用いて設定した印刷要件をドキュメントファイルに添付する。

【0043】

次に、配布者が配布者端末101の入力装置を用いて入力したパスワードを用いて、印刷要件が添付されたドキュメントファイルを暗号化して保護ドキュメントとする。

【0044】

上記の動作を図2に基づいてさらに詳しく説明する。

【0045】

まず、ドキュメント保護プログラム111の属性付与部111aは、配布者から引き渡されたドキュメントファイル（doc）に、配布者によって設定された印刷要件（req）を属性として付与し、印刷要件の付与されたドキュメントファイル（doc+req）を暗号化部111bに渡す。

【0046】

一方で暗号鍵取得部111cは、配布者によって入力されたパスワード（ku）および必要に応じて設けられたパラメータ取得部111dから得られるパラメータ（kp）に基づいて暗号鍵（k）を生成し、これを暗号化部111bに渡す。なお、パラメータ取得部111dのパラメータ（kp）はドキュメント保護プログラム111の内部に保持しておくか、要求があった場合に生成するようにする。ここで、暗号鍵（k）の生成アルゴリズムとしては、例えば、 $k=H\{ku, kp\}$ あるいは $k=D\{ku, kp\}$ が使用できる。なお、 $H\{data1, data2, \dots\}$ は $data1, data2, \dots$ のハッシュ値を計算することを意味し、 $D\{data, key\}$ はkeyでdataを復号することを意味している。

【0047】

そして、暗号化部111bは暗号鍵（k）に基づいて、印刷要件の付与されたドキュメントファイル（doc+req）を暗号化し、保護ドキュメント（enc）として出力する。式で示せば $enc=E\{(doc+req), k\}$ となる。ここで、 $E\{data, key\}$ はkeyでdataを暗号化することを意味している。

【0048】

図10に、ドキュメント印刷プログラム121の動作を示す。

【0049】

まず、ドキュメント印刷プログラム121は、ユーザがユーザ端末102の入力装置を用いて入力したパスワードを用いて保護ドキュメントを復号し、印刷要件が添付されたドキュメントファイルに復元する。次に、ドキュメント印刷プログラム121は、ドキュメ

ントファイルに設定されている印刷要件を満足するようにプリンタドライバを設定し（例えば、印刷要件として前述したPACが指定されていれば機密印刷モードに設定する）、ドキュメントを印刷する。なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0050】

ドキュメントファイルに設定されている印刷要件を満足する印刷をプリンタ103では実行できない場合、換言すると、プリンタ103が設定された印刷要件を満たす機能を備えていない場合には、ドキュメント印刷プログラム121は、その旨を示すメッセージをユーザ端末102の表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0051】

例えば、印刷要件としてPACが設定されている場合には、ドキュメント印刷プログラム121は、印刷を実行する前にPIN（個人識別番号：Personal Identification Number）の入力を要求する。この場合は、印刷実行後、プリンタ103のオペレーションパネルにおいて印刷実行前に入力したものと同一のPINが入力されるまでドキュメントのプリントアウトがプリンタ103から出力されない。このため、ドキュメントのプリントアウトがプリンタ103に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

【0052】

上記の動作を図3および図4に基づいてさらに詳しく説明する。

【0053】

まず、図3において、ドキュメント印刷プログラム121の復号部121aは、保護ドキュメント（enc）に対し、復号鍵取得部121bがパスワードおよび必要に応じて設けられたパラメータ取得部121cから得られるパラメータ（kp）から取得した復号鍵（k）を用いて復号を行う。なお、パラメータ取得部121cのパラメータ（kp）はドキュメント印刷プログラム121の内部に保持しておくか、要求があった場合に生成するようにする。ここで、復号鍵取得部121bにおける復号鍵（k）の生成アルゴリズムとしては、例えば暗号化の場合と同様に、 $k=H\{ku, kp\}$ あるいは $k=D\{ku, kp\}$ が使用できる。なお、 $H\{data1, data2, \dots\}$ は $data1, data2, \dots$ のハッシュ値を計算することを意味し、 $D\{data, key\}$ はkeyでdataを復号することを意味している。

【0054】

そして、復号部121aは復号鍵（k）によって保護ドキュメント（enc）を復号し、印刷要件の付与されたドキュメントファイル（doc+req）を得て印刷処理部121eに渡す。なお、復号を式で示せば $(doc+req)=D\{enc, k\}$ となる。ここで、 $D\{data, key\}$ はkeyでdataを復号することを意味している。一方、印刷要件取得部121dは復号されたドキュメントファイル（doc+req）から印刷要件（req）を取り出し、印刷処理部121eに渡す。

【0055】

次いで、図4において、印刷処理部121eの要件処理部121fは、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述したBDP、EBC、SLSのようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部121gに加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ121hに渡し、印刷データをプリンタ103に与えて印刷を行う。また、PACのようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ121hに印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部121iに警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部121jにログ情報を渡し、リモートサーバ等にログデータを登録させる。

【0056】

なお、以上の説明においては、図2および図3におけるパラメータ取得部111dおよびパラメータ取得部121cを任意的なものとしたが、これらを省略した場合、保護ドク

ュメントをパスワードのみで復号できることを知っている者は、ドキュメント印刷プログラム 121 を介さずに、独自にパスワードを用いて保護ドキュメントを復号することも可能ではある。

【0057】

仮にドキュメント印刷プログラム 121 を介することなく保護ドキュメントを復号した場合には、配布者が設定した印刷要件が強制されることなく、ドキュメントファイルを印刷できてしまう。

【0058】

このため、パスワードのみでドキュメントファイルを暗号化するのではなく、例えば、図 2 におけるようなパラメータ取得部 111d を設け、パスワードとドキュメント保護プログラム 111 の内部に埋め込まれている秘密鍵（パラメータ）とを合わせたもの（排他的論理和を取ったものなど）を用いてドキュメントファイルを暗号化するのが好ましい。

【0059】

この場合は、ドキュメント印刷プログラム 121 にも図 3 に示すようなパラメータ取得部 121c を設け、同一の秘密鍵（パラメータ）を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 121 のみが、保護ドキュメントを復号して印刷することが可能となる。

【0060】

さらに、プログラム内部に鍵データをそのまま格納したのでは攻撃者に察知される可能性があるため、鍵データをそのままプログラム内に保持するのではなく、必要になった際に計算して生成するようなアルゴリズムを組み込んでおくことが望ましい。その際、その生成アルゴリズムを特定されないよう、ソフトウェアの耐タンパー技術（解析されにくいようにプログラムを作成しておくことにより、攻撃者からの不正な解析からシステムを保護するための技術）を利用するといっそう安全性を高めることができる。

【0061】

〔第 2 の実施形態〕

上記の第 1 の実施形態においては、ドキュメントファイルをパスワードを用いて保護するドキュメント保護・印刷システムについて説明したが、このシステムでは、パスワードを知っているか否かでドキュメントファイルを印刷できるか否かが決まることとなる。

【0062】

しかし、実際には、「ユーザ A にはドキュメントファイルを印刷させてもよいが、ユーザ B には印刷させたくない。さらに、ユーザ C がドキュメントファイルを印刷しようとした場合には、プリントアウトに地紋を合成させるようにしたい。」といったように、ユーザ各人に応じて印刷要件を設定したい場合がある。本発明の第 2 の実施形態では、このような要求に対応できるドキュメント保護・印刷システムについて説明する。

【0063】

図 11 に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【0064】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末 201、ユーザ端末 202、プリンタ 203 およびアクセスコントロールサーバ 204 を有する。

【0065】

配布者端末 201 およびユーザ端末 202 は、第 1 の実施形態と同様に、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末 201 にはドキュメント保護プログラム 211 が、ユーザ端末 202 にはドキュメント印刷プログラム 221 がそれぞれ実装されている。

【0066】

ドキュメント保護プログラム 211 は、ドキュメントファイルに配布者端末 201 の使用者（配布者）の入力操作に応じて処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEA など）を用いてドキュメントファイルを暗号化

し、保護ドキュメントを生成する処理を行うプログラムである。図12はドキュメント保護プログラム211の構成例を示したものであり、暗号化部211aと暗号鍵取得部211bと属性付与部211cと属性登録部211dとを含んでいる。各部の機能については後の動作において説明する。

【0067】

図11に戻り、ドキュメント印刷プログラム221は、ユーザ端末202の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号するとともに処理要件の一部として設定されている印刷要件に応じた印刷処理をプリンタ203に実行させる処理を行うプログラムである。図13はドキュメント印刷プログラム221の構成例を示したものであり、復号部221aと復号鍵取得部221bと印刷要件取得部221cと印刷処理部221dとを含んでいる。また、図14は図13における印刷処理部221dの構成例を示したものであり、要件処理部221eとドキュメント加工部221fとプリンタドライバ221gと警告表示部221hとログ記録部221iとを含んでいる。各部の機能については後の動作において説明する。

【0068】

図11に戻り、アクセスコントロールサーバ204は、ユーザがドキュメントにアクセス（例えば、印刷）しようとする場合に、ドキュメント印刷プログラム221からの要求に応じてアクセス制御リスト（Access Control List：ACL）を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

【0069】

アクセスコントロールサーバ204には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース241と、ユーザ各人ごとに設定された処理要件（印刷処理の要件を特に印刷要件という）を含むACLが登録されるACLデータベース242とが接続されている。

【0070】

図15はアクセスコントロールサーバ204の構成例を示したものであり、属性DB登録部204aとユーザ認証部204bとアクセス権限確認部204cと印刷要件取得送付部204dとを含んでいる。各部の機能については後の動作において説明する。

【0071】

なお、ACLの構造例を図16に示す。ACLはユーザ名（User Name）、アクセスタイプ（Access Type）、許可情報（Permission）および処理要件（Requirement）をパラメータとして構成される。そして、このACLは、図17に示すように、後述するドキュメントID（Document ID）および暗号鍵（Key）と関連付けられて一つのレコードとしてACLデータベース242に記録保持される。

【0072】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初にシステム全体の動作について説明する。

【0073】

図11において、配布者は、配布者端末201を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【0074】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末201の入力装置を操作してドキュメントファイルをドキュメント保護プログラム211に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム211は、ACLの設定を配布者に要求する。例えば、ドキュメント保護プログラム211は、配布者端末201の表示装置にメッセージを表示するなどして、ACLの設定を要求する。図18はACLの設定を要求する画面の例を示したものであり、ユーザ名、アクセス許可、印刷要件の設

定が行えるようになっている。すなわち、ACLのエントリとなるグループまたはユーザを追加し、そのグループまたはユーザに割り当てるアクセス権限を指定する。その際、必要に応じて印刷要件を指定することができ、印刷要件として設定可能なものの中から選択（チェック）を行い、更に補足情報が必要なものについては入力を行う。図ではウォーターマークの文字列として「CONFIDENTIAL」を指定している。そして、暗号化ボタンを押すことにより設定内容が取り込まれる。なお、この画面では保護するドキュメントファイルを指定することもできるようになっている。

【0075】

配布者が配布者端末201の入力装置を介してACLを設定すると、ドキュメント保護プログラム211はこれを取得する。

【0076】

ACLを取得したドキュメント保護プログラム211は、ドキュメントファイルごとに固有のドキュメントID（Document ID）と暗号化および復号に使用する暗号鍵（Key）とを生成し、ACLをこれらに関連付けてアクセスコントロールサーバ204へ送信し、ACLデータベース242への登録を要求する。

【0077】

また、ドキュメント保護プログラム211は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメントIDを付加して保護ドキュメントを生成する。

【0078】

配布者は、ドキュメント保護プログラム211が生成した保護ドキュメントをユーザに受け渡す。

【0079】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末202に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末202に読み取らせても良いし、ユーザ端末202が配布者端末201と通信可能である場合には、通信網を介して配布者端末201から保護ドキュメントを取得するようにしてもよい。

【0080】

ユーザが、ユーザ端末202の入力装置を介してドキュメント印刷プログラム221に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム221は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム221は、ユーザ端末202の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。図19はユーザ名（ユーザID）とパスワードを要求する画面の例を示したものであり、キーボード等によって入力が行えるようになっている。

【0081】

ドキュメント印刷プログラム221は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ204へ送信して、ユーザ認証を要求する。

【0082】

アクセスコントロールサーバ204は、ドキュメント印刷プログラム221から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0083】

ユーザを特定すると、アクセスコントロールサーバ204は、ACLデータベース242を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかを取得する。

【0084】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ204は、その旨を示す認証情報とともに、保護ドキュメントを復号するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末202を介して

ドキュメント印刷プログラム 2 2 1 に通知する。

【0085】

アクセスコントロールサーバ 2 0 4 から認証情報とともに、暗号鍵と印刷要件とを取得したドキュメント印刷プログラム 2 2 1 は、暗号鍵を用いて保護ドキュメントを復号してドキュメントファイルに復元する。

【0086】

そしてドキュメント印刷プログラム 2 2 1 は、印刷要件を満たすようにプリンタ 2 0 3 に印刷処理を実行させる。例えば、ドキュメントファイルに前述した B D P が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【0087】

これにより、ドキュメントファイルを印刷する際に、配布者がユーザ各人に対して設定した印刷要件を強制することが可能となる。

【0088】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 2 1 1 およびアクセスコントロールサーバ 2 0 4 の動作、および保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 2 2 1 およびアクセスコントロールサーバ 2 0 4 の動作についてさらに詳しく説明する。

【0089】

図 2 0 に、ドキュメント保護プログラム 2 1 1 が保護ドキュメントを生成する際の動作を示す。ドキュメント保護プログラム 2 1 1 は、配布者端末 2 0 1 の入力装置における配布者の入力操作によってドキュメントファイルと A C L とを取得すると、ドキュメントファイルを暗号化および復号するための暗号鍵を生成する。そして、ドキュメント保護プログラム 2 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0090】

さらにドキュメント保護プログラム 2 1 1 は、ドキュメントファイルごとに固有のドキュメント I D を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【0091】

保護ドキュメントを生成した後、ドキュメント保護プログラム 2 1 1 は配布者端末 2 0 1 の通信機能を用いて、暗号鍵と A C L とドキュメント I D とをアクセスコントロールサーバ 2 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 2 0 4 に要求する。

【0092】

暗号鍵と A C L とドキュメント I D とをドキュメント保護プログラム 2 1 1 から受け渡されたアクセスコントロールサーバ 2 0 4 は、図 1 7 に示したように、これらに関連付けて一つのレコードとして A C L データベース 2 4 2 に記録保持する。

【0093】

上記の動作を図 1 2 および図 1 5 に基づいてさらに詳しく説明する。

【0094】

まず、図 1 2 において、ドキュメント保護プログラム 2 1 1 の暗号化部 2 1 1 a は、配布者から引き渡されたドキュメントファイルに対し、暗号鍵取得部 2 1 1 b が生成した暗号鍵を用いて暗号化を行い、この暗号化ドキュメントを属性付与部 2 1 1 c に渡す。

【0095】

属性付与部 2 1 1 c はドキュメント I D を生成し、暗号化部 2 1 1 a から渡された暗号化ドキュメントにドキュメント I D を付与して保護ドキュメントとして出力する。

【0096】

また、属性登録部 2 1 1 d は配布者から A C L を受け取るとともに、暗号鍵取得部 2 1 1 b から暗号鍵を、属性付与部 2 1 1 c からドキュメント I D をそれぞれ受け取り、アクセスコントロールサーバ 2 0 4 に対してこれらのドキュメント I D、暗号鍵、A C L を渡して登録を要求する。

【0097】

次いで、図 1 5 において、アクセスコントロールサーバ 2 0 4 の属性 DB 登録部 2 0 4 a は、渡されたドキュメント ID、暗号鍵、ACL を ACL データベース 2 4 2 に登録する。

【0 0 9 8】

なお、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメント保護プログラム 2 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 2 0 4 や不図示のサーバなどで行っても良い。

【0 0 9 9】

また、配布者端末 2 0 1 とアクセスコントロールサーバ 2 0 4 との間が専用回線ではなくネットワークを介して接続されており、暗号鍵などを送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0 1 0 0】

ドキュメント保護プログラム 2 1 1 がアクセスコントロールサーバ 2 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしてもよい。その場合、アクセスコントロールサーバ 2 0 4 は、例えば「register(String docId, byte[] key, byte[] acl)」のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTPS の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【0 1 0 1】

次に、ドキュメント印刷プログラム 2 2 1 が保護ドキュメントを印刷する際の動作について説明する。

【0 1 0 2】

図 2 1 に、保護ドキュメントを印刷する際のドキュメント印刷プログラム 2 2 1 およびアクセスコントロールサーバ 2 0 4 の動作の流れを示す。

【0 1 0 3】

ドキュメント印刷プログラム 2 2 1 は、ユーザ端末 2 0 2 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

【0 1 0 4】

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print” となる。）とをアクセスコントロールサーバ 2 0 4 へ送信して、アクセス権限があるか否かのチェックを要求する。なお、図 2 2 はアクセスコントロールサーバ 2 0 4 への SOAP による問い合わせの例を示す図であり、ユーザ名 (userId) とドキュメント ID (docId) とアクセスタイプ (accessType) とを渡してアクセスが許可されているかを問い合わせる SOAP メッセージ (isAllowed) を送付し、その結果 (isAllowedResponse) を受け取っている例である。結果には、許可されているということ (allowed が true) と要件 (requirements) とが含まれている。

【0 1 0 5】

アクセスコントロールサーバ 2 0 4 は、ドキュメント印刷プログラム 2 2 1 からユーザ名とパスワードとドキュメント ID とアクセスタイプとを取得すると、ユーザデータベース 2 4 1 に登録されている情報を参照し、ユーザ認証を行う。

【0 1 0 6】

換言すると、アクセスコントロールサーバ 2 0 4 は、ユーザデータベース 2 4 1 に登録されている情報を参照し、ドキュメント印刷プログラム 2 2 1 から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース 2 4 1 に組として登録されているか否かを判断する。

【0 1 0 7】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム 2 2 1 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 2 4 1 に登録されていない場合）、アクセスコントロールサーバ 2 0 4 は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」としてユーザ端末 2 0 2 へ送信し、ドキュメント印刷プログラム 2 2 1 へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 2 2 1 へ受け渡すようにしてもよい。

【0 1 0 8】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ 2 0 4 は、ACL データベース 2 4 2 に格納されているレコードのうち、ドキュメント印刷プログラム 2 2 1 から取得した情報に含まれるドキュメント ID に関するレコードを読み出す。

【0 1 0 9】

アクセスコントロールサーバ 2 0 4 は、読み出したレコードに含まれる ACL を取得し、ドキュメント印刷プログラム 2 2 1 から取得したユーザ名およびアクセスタイプに基づいて、ACL から許可情報および印刷要件を取得する。

【0 1 1 0】

換言すると、アクセスコントロールサーバ 2 0 4 は、ユーザ名とアクセスタイプとに基づいて、予め ACL に設定されている許可情報と印刷要件とを取得する。

【0 1 1 1】

ACL から取得した許可情報が「許可」である場合、アクセスコントロールサーバ 2 0 4 は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともにユーザ端末 2 0 2 へ送信してドキュメント印刷プログラム 2 2 1 に受け渡す。

【0 1 1 2】

一方、ACL から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ 2 0 4 は、許可情報のみをユーザ端末 2 0 2 へ送信してドキュメント印刷プログラム 2 2 1 に受け渡す。

【0 1 1 3】

アクセスコントロールサーバ 2 0 4 から許可情報を受け渡されたドキュメント印刷プログラム 2 2 1 は、取得した許可情報を参照し、「不許可」である場合には、ユーザ端末 2 0 2 の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

【0 1 1 4】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号してドキュメントファイルに復元する。

【0 1 1 5】

また、ドキュメント印刷プログラム 2 2 1 は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PAC が指定されていれば機密印刷モードに設定する）、プリンタ 2 0 3 にドキュメントの印刷処理を実行させる。

【0 1 1 6】

なお、必要があれば、ユーザ端末 2 0 2 の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0 1 1 7】

アクセスコントロールサーバ 2 0 4 から取得した印刷要件を満足する印刷をプリンタ 2 0 3 では実行できない場合、換言すると、プリンタ 2 0 3 が ACL に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0 1 1 8】

上記の動作を図 1 3 ～図 1 5 に基づいてさらに詳しく説明する。

【0 1 1 9】

まず、図 1 3 において、ドキュメント印刷プログラム 2 2 1 の復号鍵取得部 2 2 1 b は

アクセスコントロールサーバ 2 0 4 に対してアクセス権の確認を行う。

【0 1 2 0】

確認の問い合わせを受けたアクセスコントロールサーバ 2 0 4 は、図 1 5 において、ユーザ認証部 2 0 4 b がユーザデータベース 2 4 1 を参照してユーザ認証を行い、認証結果をドキュメント印刷プログラム 2 2 1 に通知する。また、ユーザ認証に成功した場合、アクセス権限確認部 2 0 4 c が A C L データベース 2 4 2 を参照して許可情報および復号鍵を取得するとともに、印刷要件取得送付部 2 0 4 d が印刷要件を取得し、ドキュメント印刷プログラム 2 2 1 に通知する。なお、図 1 5 ではいったん認証結果を返してから再び認証結果を渡すようにしているが、これを一度に実行してもよい。また、許可情報、復号鍵および印刷要件を別々に返すようにしているが、これらを一度に返すようにしてもよい。

【0 1 2 1】

図 1 3 において、復号鍵取得部 2 2 1 b はアクセス権の確認ができた場合にアクセスコントロールサーバ 2 0 4 から復号鍵を得て、これを復号部 2 2 1 a に渡す。また、印刷要件取得部 2 2 1 c はアクセスコントロールサーバ 2 0 4 から印刷要件を取得し、印刷処理部 2 2 1 d に渡す。

【0 1 2 2】

復号部 2 2 1 a は復号鍵取得部 2 2 1 b から取得した復号鍵を用いて保護ドキュメントを復号し、ドキュメントファイルを得て印刷処理部 2 2 1 d に渡す。

【0 1 2 3】

次いで、図 1 4 において、印刷処理部 2 2 1 d の要件処理部 2 2 1 e は、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述した B D P、E B C、S L S のようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部 2 2 1 f に加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ 2 2 1 g に渡し、印刷データをプリンタ 2 0 3 に与えて印刷を行う。また、P A C のようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ 2 2 1 g に印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部 2 2 1 h に警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部 2 2 1 i にログ情報を渡し、リモートサーバ等にログデータを登録させる。

【0 1 2 4】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、A C L データベース 2 4 2 に登録されている A C L の内容を配布者端末 2 0 1 やアクセスコントロールサーバ 2 0 4 における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

【0 1 2 5】

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0 1 2 6】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 2 2 1 に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号することも可能ではある。この場合は、A C L として設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0 1 2 7】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 2 1 1 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。この場合は、ドキュメント印刷プログラム 2 2 1 にも同一の秘密鍵を埋め込んでおくこと

で、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 221 のみが、保護ドキュメントを復号して印刷することが可能となる。

【0128】

図 23 および図 24 は上述したような内部に秘密鍵を埋め込んでおくタイプの構成例を示したものであり、図 23 はドキュメント保護プログラム 211 の構成例を示し、図 24 はドキュメント印刷プログラム 221 の構成例のうち復号に関する部分のみを示している。なお、この例は、単に内部に秘密鍵を埋め込んでおくだけではなく、乱数を導入して不正アクセスに対しより強化している。

【0129】

図 23 において、ドキュメント保護プログラム 211 は暗号化部 211a と暗号鍵取得部 211b と属性付与部 211c と属性登録部 211d とパラメータ取得部 211e とを含んでいる。

【0130】

動作にあつては、パラメータ取得部 211e はパラメータ (kp) を生成し、暗号鍵取得部 211b に渡す。なお、パラメータ (kp) はドキュメント保護プログラム 211 の内部に保持しておくか、要求があつた場合に生成するようにする。

【0131】

暗号鍵取得部 211b はパラメータ取得部 211e からパラメータ (kp) を受け取った上で、二つの乱数 (kd) (ks) を生成し、暗号鍵 (k) を式 $k = H\{ks, kp, kd\}$ あるいは $k = D\{kd, D\{ks, kp\}\}$ で計算して生成し、暗号鍵 (k) を暗号化部 211a に、乱数 (kd) を属性付与部 211c に、乱数 (ks) を属性登録部 211d にそれぞれ渡す。なお、 $H\{data1, data2, \dots\}$ は $data1, data2, \dots$ のハッシュ値を計算することを意味し、 $D\{data, key\}$ は key で data を復号することを意味している。

【0132】

暗号化部 211a は配布者から引き渡されたドキュメントファイル (doc) に対し、暗号鍵取得部 211b から取得した暗号鍵 (k) を用いて暗号化を行い、暗号化されたドキュメント (enc) を属性付与部 211c に渡す。式で示せば $enc = E\{doc, k\}$ となる。なお、 $E\{data, key\}$ は key で data を暗号化することを意味している。

【0133】

次いで、属性付与部 211c はドキュメント ID (id) を生成し、暗号化されたドキュメント (enc) にそのドキュメント ID (id) と暗号鍵取得部 211b から渡された乱数 (kd) を付与して保護ドキュメント ($enc + id + kd$) を出力する。また、属性付与部 211c は生成したドキュメント ID (id) を属性登録部 211d に渡す。

【0134】

属性登録部 211d は、属性付与部 211c から渡されたドキュメント ID (id) と暗号鍵取得部 211b から渡された乱数 (ks) と配布者から取得した ACL (attr) とをアクセスコントロールサーバ 204 に通知し、登録を要求することになる。

【0135】

復号にあつては、図 24 において、復号鍵取得部 221b は保護ドキュメントから乱数 (kd) を取得するとともに、パラメータ取得部 221j からドキュメント印刷プログラム 221 の内部に保持してある、あるいは要求に応じて生成したパラメータ (kp) を取得し、さらにアクセスコントロールサーバ 204 から乱数 (ks) を取得し、暗号化の場合と同様に式 $k = H\{ks, kp, kd\}$ あるいは $k = D\{kd, D\{ks, kp\}\}$ で計算して復号鍵 (暗号鍵) (k) を得る。

【0136】

そして、復号部 221a は暗号化されたドキュメント (enc) を復号鍵 (k) で復号し、ドキュメントファイル (doc) を得る。

【0137】

図 23 および図 24 は、アクセスコントロールサーバ 204 に登録される乱数 (ks) と保護ドキュメント内の乱数 (kd) とドキュメント保護プログラム 211 もしくはドキュメ

ント印刷プログラム 2 2 1 内から取得されるパラメータ (kp) とに基づいて暗号鍵 (復号鍵) (k) を生成する方式であるが、こうすることでアクセスコントロールサーバ 2 0 4 が悪意のあるユーザによって不正アクセスされて乱数 (ks) が知られてしまった場合であっても、乱数 (kd) やパラメータ (kp) が知られなければ保護ドキュメントを復号できないことになる。なお、アクセスコントロールサーバ 2 0 4 が不正アクセスされないように十分にガードされている環境にあっては、乱数 (ks) をそのまま暗号鍵 (復号鍵) (k) として使用してもよい。

【0 1 3 8】

一方、これまで説明してきた第 2 の実施形態では、印刷要件をアクセスコントロールサーバ 2 0 4 にのみ格納するものとしてきたが、そのような形式に限定されず、保護ドキュメントに含めるようにしてもよい。例えば、ユーザによらずドキュメントファイルに対して必ず指定するような印刷要件については保護ドキュメントの中に含めるようにしてもよい。

【0 1 3 9】

図 2 5 は、印刷要件を保護ドキュメントに含める第一印刷要件と、アクセスコントロールサーバ 2 0 4 に格納される第二印刷要件とに分けた場合のドキュメント印刷プログラム 2 2 1 の構成例を示したものであり、印刷要件取得部 2 2 1 c においてアクセスコントロールサーバ 2 0 4 から第二印刷要件を取得するとともに、復号部 2 2 1 a において保護ドキュメントから第一印刷要件を取得し、第一印刷要件および第二印刷要件に基づいて印刷処理部 2 2 1 d で印刷処理を行うようにしている。その他は図 1 3 に示したドキュメント印刷プログラム 2 2 1 と同様である。

【0 1 4 0】

また、本実施形態においては、ドキュメント印刷プログラム 2 2 1 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 2 2 1 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat (R) の Plug-in としてポータブルドキュメントファイル (Portable Document Format : P D F File) の表示、編集および印刷の機能を実現することが可能である。

【0 1 4 1】

図 2 6 に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。これらについて第 2 の実施形態におけるシステム構成を例として具体的に説明する。

【0 1 4 2】

まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 2 2 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 2 2 1 の動作を図 2 7 に示す。

【0 1 4 3】

(1) ドキュメント印刷プログラム 2 2 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 2 8 に示すように、プリントダイアログを表示させた後に個人識別番号 (Personal Identification Number : P I N) を入力するダイアログをユーザ端末 2 0 2 の表示装置に表示させ、ユーザに P I N の入力を要求する。

【0 1 4 4】

(2) ユーザ端末 2 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 2 2 1 は、これをプリンタドライバに設定し、印刷を指示する。

【0 1 4 5】

プリンタドライバは、ドキュメントから Postscript などの P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバはさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリンタ 2 0 3 に送る。

【 0 1 4 6 】

プリンタ 2 0 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 2 0 3 内部の記憶装置（HDD など）に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 2 0 3 のオペレーションパネルを介して入力すると、プリンタ 2 0 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながら P D L データに従って印刷出力する。

【 0 1 4 7 】

（3）プリンタドライバに P I N が設定できない、すなわち、プリンタ 2 0 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【 0 1 4 8 】

このようにすることで、印刷実行後、プリンタ 2 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 2 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 2 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 2 0 3 とのやりとりを S S L で保護してもよい。

【 0 1 4 9 】

また、ドキュメント印刷プログラム 2 2 1 を Windows（R）Domain のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows（R）Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 2 0 3 へ送付するようにする。プリンタ 2 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで Windows（R）Domain のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（R）Domain に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

【 0 1 5 0 】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プログラム 2 2 1 の動作について説明する。

【 0 1 5 1 】

（1）ドキュメント印刷プログラム 2 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ（又は、二次元コード）のデータを生成する。

【 0 1 5 2 】

（2）ドキュメント印刷プログラム 2 2 1 は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリンタ 2 0 3 に印刷を指示する。

【 0 1 5 3 】

（3）プリンタドライバに E B C が設定できない、すなわち、プリンタ 2 0 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 1 5 4 】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にアクセスコントロールサーバ 2 0 4 でハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【 0 1 5 5 】

次に、印刷要件として B D P が設定されている場合のドキュメント印刷プログラム 2 2 1 の動作について説明する。

【 0 1 5 6 】

(1) ドキュメント印刷プログラム 2 2 1 は、B D P が設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro, 2002/08/04 23:47:10）。

【 0 1 5 7 】

(2) ドキュメント印刷プログラム 2 2 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

【 0 1 5 8 】

(3) ドキュメント印刷プログラム 2 2 1 は、生成した地紋画像をスタンプとしてプリンタドライバにセットし、プリンタ 2 0 3 にドキュメントの印刷を指示する。

【 0 1 5 9 】

(4) プリンタドライバに B D P が設定できない場合、すなわちプリンタ 2 0 3 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 1 6 0 】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋画像として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、E B C をサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【 0 1 6 1 】

次に、印刷要件として S L S が設定されている場合のドキュメント印刷プログラム 2 2 1 の動作について説明する。

【 0 1 6 2 】

(1) ドキュメント印刷プログラム 2 2 1 は、S L S が設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secret ならば「極秘」のマークなど）を選択する。

【 0 1 6 3 】

(2) 選択した画像のデータを、スタンプとしてプリンタドライバにセットし、プリンタ 2 0 3 に印刷を指示する。

【 0 1 6 4 】

(3) プリンタドライバに S L S をセットできない場合、すなわち、プリンタ 2 0 3 が S L S をサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 1 6 5 】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【 0 1 6 6 】

上記の各例は、あくまでも印刷要件の例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

【 0 1 6 7 】

さらに付言すると、印刷要件には、機能を制限・禁止するものと、機能を強制的に使用させるもの、加えて通常の印刷条件指定などを含めることができる。機能を制限・禁止する例としては、機密文書原本と区別をするために特別なユーザのみカラーでの印刷を許可

して、他のユーザはグレースケールでの印刷のみを許可するように制限するための印刷要件などである。機能を強制的に使用させる例としては、機密印刷モードを強制的に使用するような印刷要件や、ログを強制的に記録するような印刷要件、印刷紙面に印刷したユーザの名前を強制的に印字するような印刷要件、ウォーターマークを強制的に印刷する印刷要件、地紋を強制的に印刷する印刷要件などである。通常の印刷条件を指定する例としては、用紙設定として A 4 を指定する印刷要件、再生紙トレイを使用する印刷要件、両面印刷を指定する印刷要件などである。

【0168】

また、これまで印刷要件の表現形式として RAD、PAC といったキーワードを用いて説明してきたが、そのようなキーワードでなくとも、例えば、プリンタドライバに設定する設定ファイルのデータそのものや、プリントデータに挿入するページ記述言語で表現したデータ、画面に表示する文字列そのもの、処理すべき要件の内容をスクリプト言語で記述したデータのようなものを用いて印刷要件を表現して規定するようにしても良い。すなわち、印刷要件の表現をキーワードのようなものに限定するものではない。

【0169】

このように、プリンタ 203 がサポートする様々なセキュリティ機能を利用してセキュリティポリシーに沿った印刷要件を設定することによって、プリンタ 203 のセキュリティ機能が無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは他の実施形態のシステム構成においても同様である。

【0170】

一方、これまでの説明において、保護対象はドキュメント全体であるように記述してきたが、ドキュメントの中に保護対象となる部分（セグメントと呼ぶ）と、保護対象としない部分が混在していても良い。例えば、図 29 に示すように、保護セグメントが複数保護ドキュメント内に存在していても良い。この場合、保護セグメントごとに異なるセグメント ID をつけ、これまでの説明におけるドキュメント ID をセグメント ID と読みかえれば、同じ原理で保護セグメントごとに印刷を含むアクセスの制御が可能になる。実際には、保護セグメントの先頭と末尾には、そこから保護セグメントが開始することを示しそこで保護セグメントが終了することを示すマーカーのようなものをつける必要がある。そういったマーカーの入れ方については、MIME のマルチパートセパレータなどの従来技術を用いることができる。

【0171】

また、これまではドキュメント保護プログラムが配布者端末に配置されるような実施例に基づいて説明してきたが、ドキュメント保護プログラム本体はリモートサーバ上に配置するようにしても良い。例えば図 11 の配布者端末 201、ドキュメント保護プログラム 211 およびアクセスコントロールサーバ 204 の関係は、図 30 に示すように変形することができる。このように配置することにより、ドキュメント保護プログラムがインストールされていない端末からでもリモートサーバにドキュメントと必要なパラメータを送付して保護ドキュメントを取得することができる。

【0172】

なお、上述した各実施形態は、本発明の好適な実施の例であり、本発明はこれらに限定されることはない。

【0173】

例えば、上記各実施形態においては、配布者端末とユーザ端末とが別個の装置である場合を例に説明を行ったが、これらは同一の装置を共用するような構成であっても構わない。

【0174】

また、上記各実施形態では、ドキュメント印刷プログラムが実装されたユーザ端末を、ユーザが直接操作する場合を例に説明を行ったが、これに限定されるものではない。例えば、ドキュメント印刷プログラムがサーバに実装されており、ユーザがユーザ端末を操作しネットワークを介してドキュメント印刷プログラムを実行させる構成であってもよい。

【0175】

また、ユーザ認証の方法は、ユーザ名とパスワードとを用いる方法に限定されることなく、スマートカードを用いたPKIベースの認証方法を適用してもよい。

【0176】

このように、本発明は様々な変形が可能である。

【0177】

さらに、上記の説明では「プリンタ」という用語が使われているが、これは狭義のプリンタ専用機に限らず、コピー、ファクシミリ、これらの複合・融合された機器等、すなわち印刷機能を有するすべての機器を意味するものである。

【図面の簡単な説明】

【0178】

【図1】本発明を好適に実施した第1の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図2】ドキュメント保護プログラムの構成例を示す図である。

【図3】ドキュメント印刷プログラムの構成例を示す図である。

【図4】印刷処理部の構成例を示す図である。

【図5】パスワードと印刷要件の設定を要求する画面の例を示す図である。

【図6】保護ドキュメントの保存場所を問い合わせる画面の例を示す図である。

【図7】パスワードを要求する画面の例を示す図である。

【図8】ユーザ端末の表示装置上に表示される確認画面の例を示す図である。

【図9】第1の実施形態にかかるドキュメント保護プログラムの動作を示す図である。

【図10】第1の実施形態にかかるドキュメント印刷プログラムの動作を示す図である。

【図11】本発明を好適に実施した第2の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図12】ドキュメント保護プログラムの構成例を示す図である。

【図13】ドキュメント印刷プログラムの構成例を示す図である。

【図14】印刷処理部の構成例を示す図である。

【図15】アクセスコントロールサーバの構成例を示す図である。

【図16】ACLの構成例を示す図である。

【図17】ACLデータベースに記録される情報の構造例を示す図である。

【図18】ACLの設定を要求する画面の例を示す図である。

【図19】ユーザ名（ユーザID）とパスワードを要求する画面の例を示す図である。

【図20】第2の実施形態にかかるドキュメント保護プログラムの動作を示す図である。

【図21】第2の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図22】アクセスコントロールサーバへのSOAPによる問い合わせの例を示す図である。

【図23】ドキュメント保護プログラムの構成例を示す図である。

【図24】復号の様子を示す図である。

【図25】ドキュメント印刷プログラムの構成例を示す図である。

【図26】プリンタが備えるセキュリティ機能の例を示す図である。

【図27】PACが設定されたドキュメントを印刷する際の処理を示す図である。

【図28】PIN入力のダイアログを示す図である。

【図29】ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図である。

【図30】ドキュメント保護プログラムをリモートサーバ上に配置した状態を示す図

である。

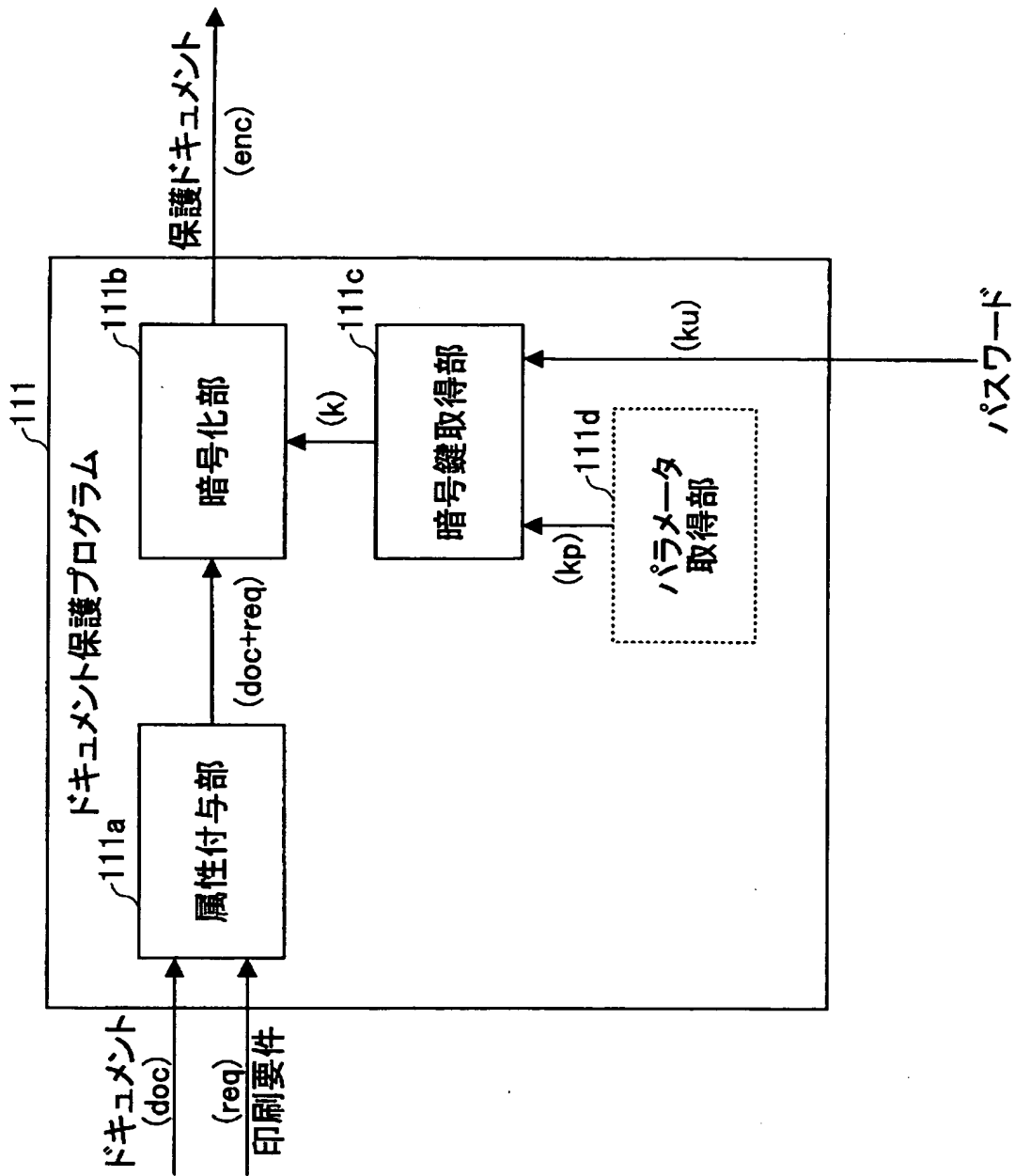
【符号の説明】

【 0 1 7 9 】

1 0 1	配布者端末
1 0 2	ユーザ端末
1 0 3	プリンタ
1 1 1	ドキュメント保護プログラム
1 2 1	ドキュメント印刷プログラム
1 1 1 a	属性付与部
1 1 1 b	暗号化部
1 1 1 c	暗号鍵取得部
1 1 1 d	パラメータ取得部
1 2 1 a	復号部
1 2 1 b	復号鍵取得部
1 2 1 c	パラメータ取得部
1 2 1 d	印刷要件取得部
1 2 1 e	印刷処理部
1 2 1 f	要件処理部
1 2 1 g	ドキュメント加工部
1 2 1 h	プリンタドライバ
1 2 1 i	警告表示部
1 2 1 j	ログ記録部
2 0 1	配布者端末
2 0 2	ユーザ端末
2 0 3	プリンタ
2 0 4	アクセスコントロールサーバ
2 1 1	ドキュメント保護プログラム
2 2 1	ドキュメント印刷プログラム
2 4 1	ユーザデータベース
2 4 2	A C L データベース
2 1 1 a	暗号化部
2 1 1 b	暗号鍵取得部
2 1 1 c	属性付与部
2 1 1 d	属性登録部
2 1 1 e	パラメータ取得部
2 2 1 a	復号部
2 2 1 b	復号鍵取得部
2 2 1 c	印刷要件取得部
2 2 1 d	印刷処理部
2 2 1 e	要件処理部
2 2 1 f	ドキュメント加工部
2 2 1 g	プリンタドライバ
2 2 1 h	警告表示部
2 2 1 i	ログ記録部
2 2 1 j	パラメータ取得部
2 0 4 a	属性 D B 登録部
2 0 4 b	ユーザ認証部
2 0 4 c	アクセス権限確認部
2 0 4 d	印刷要件取得送付部

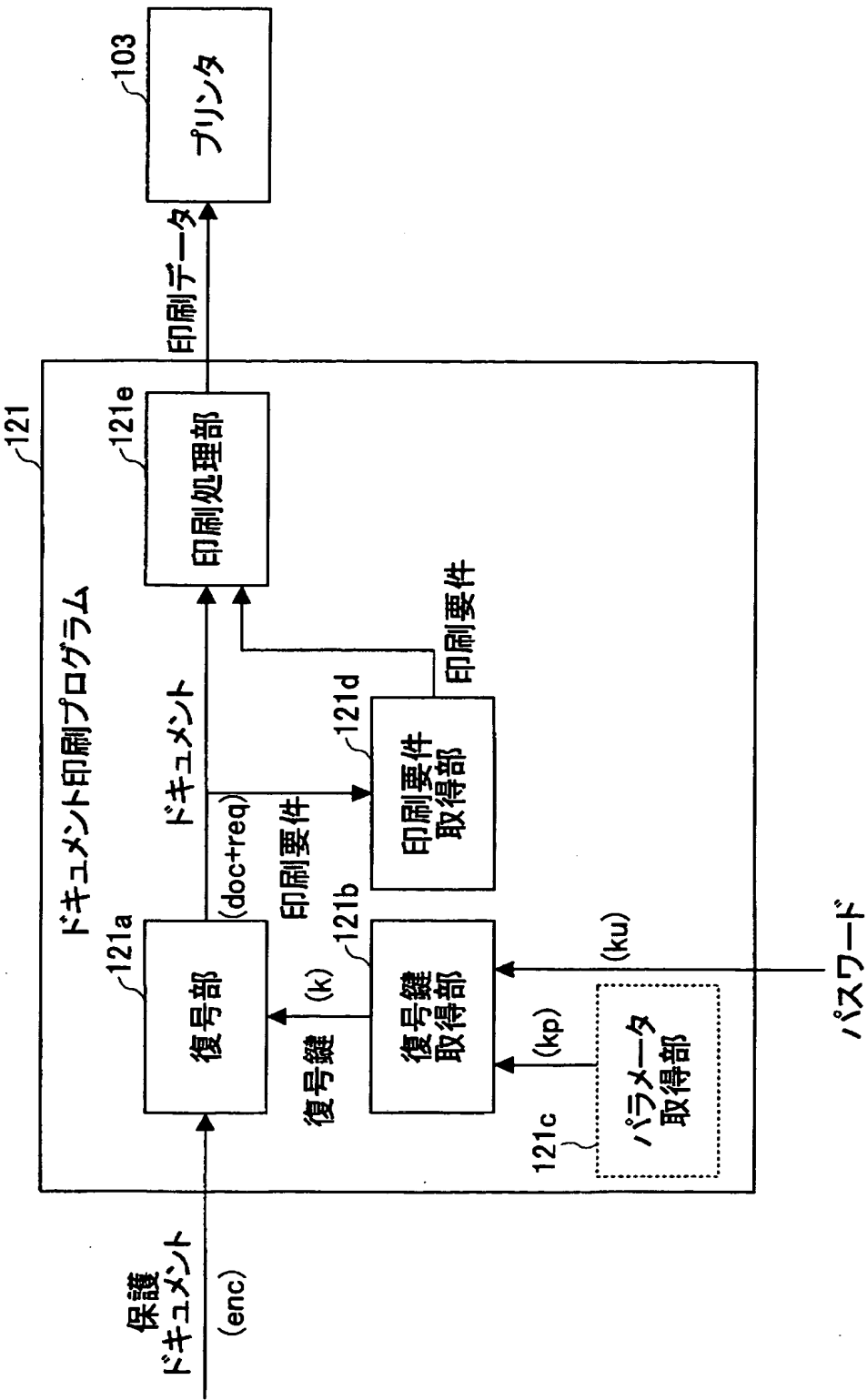
【図 2】

ドキュメント保護プログラムの構成例を示す図



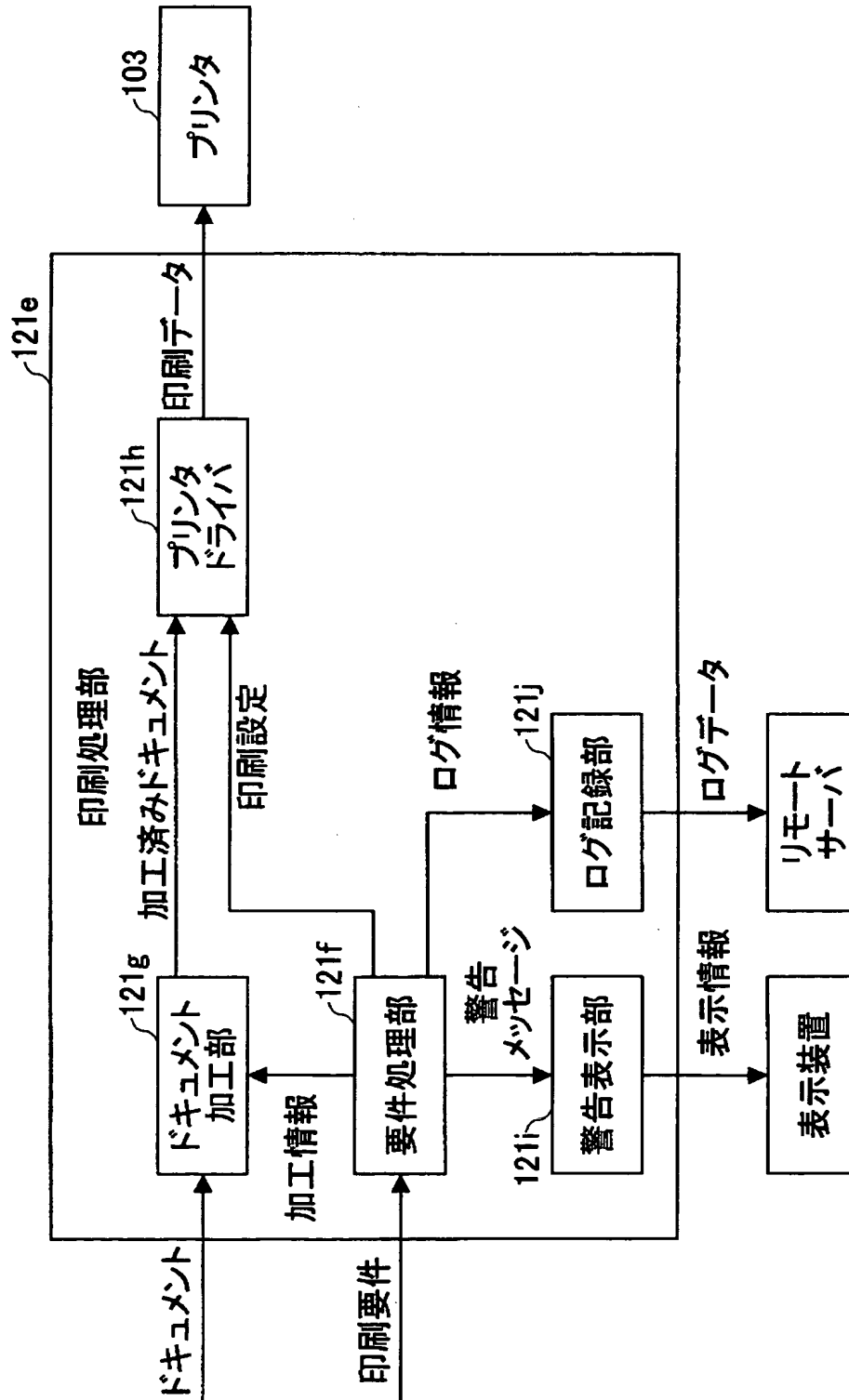
【図 3】

ドキュメント印刷プログラムの構成例を示す図



【図 4】

印刷処理部の構成例を示す図



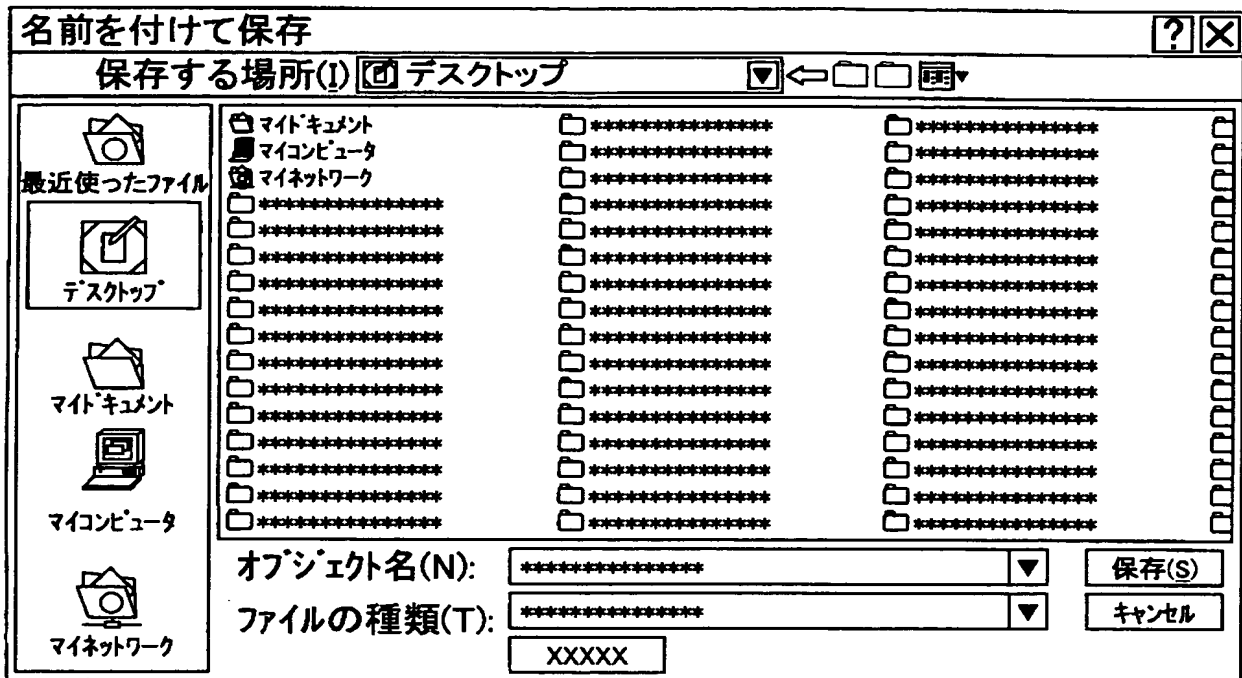
【図 5】

パスワードと印刷要件の設定を要求する画面の例を示す図

パスワード:	<input type="text" value="*****"/>
印刷セキュリティ:	
印刷許可	<input checked="" type="checkbox"/>
ただし、	
機密印刷	<input type="checkbox"/>
マル秘スタンプ	<input type="checkbox"/>
ウォーターマーク	<input checked="" type="checkbox"/> <input type="text" value="CONFIDENTIAL"/>
地紋印刷	<input type="checkbox"/> <input type="text"/>
ファイル:	<input type="text" value="C:\My Documents\sample.doc"/> <input type="button" value="参照"/>
<input type="button" value="暗号化"/>	

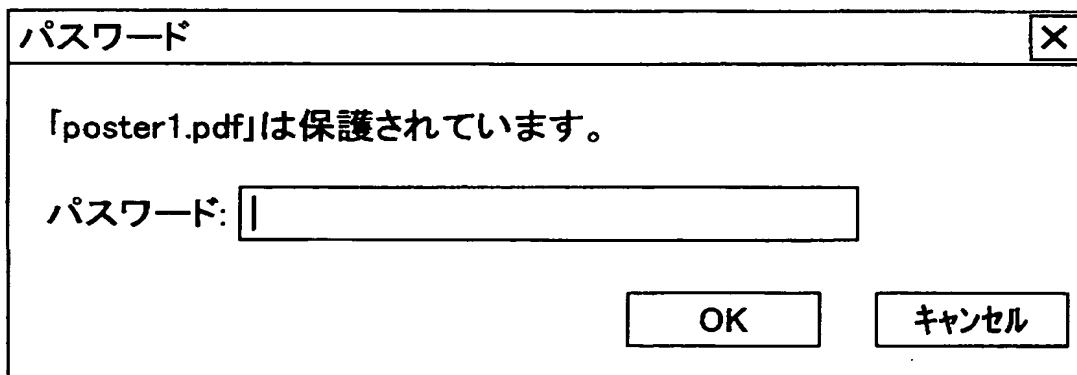
【図 6】

保護ドキュメントの保存場所を問い合わせる画面の例を示す図



【図 7】

パスワードを要求する画面の例を示す図



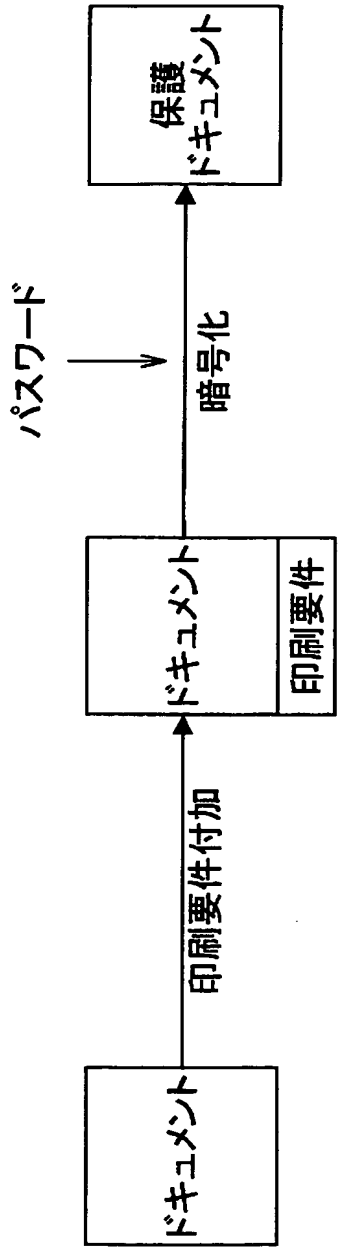
【図 8】

ユーザ端末の表示装置上に表示される確認画面の例を示す図

<p>印刷セキュリティ</p> <p>このドキュメントには以下の印刷要件が指定されています。</p> <div>機密印刷 ウォーターマーク</div>	<p>プリンタ</p> <p>以下のプリンタで印刷要件を処理できます。</p> <div><div>▼</div><div>Network Printer A Network Printer B Local Printer E</div></div>	<div>印刷</div> <div>キャンセル</div>
---	---	--------------------------------

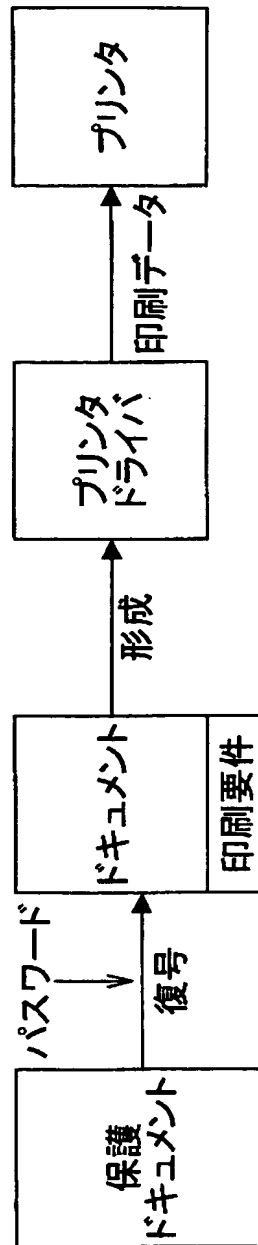
【図 9】

第1の実施形態にかかるドキュメント保護プログラムの動作を示す図



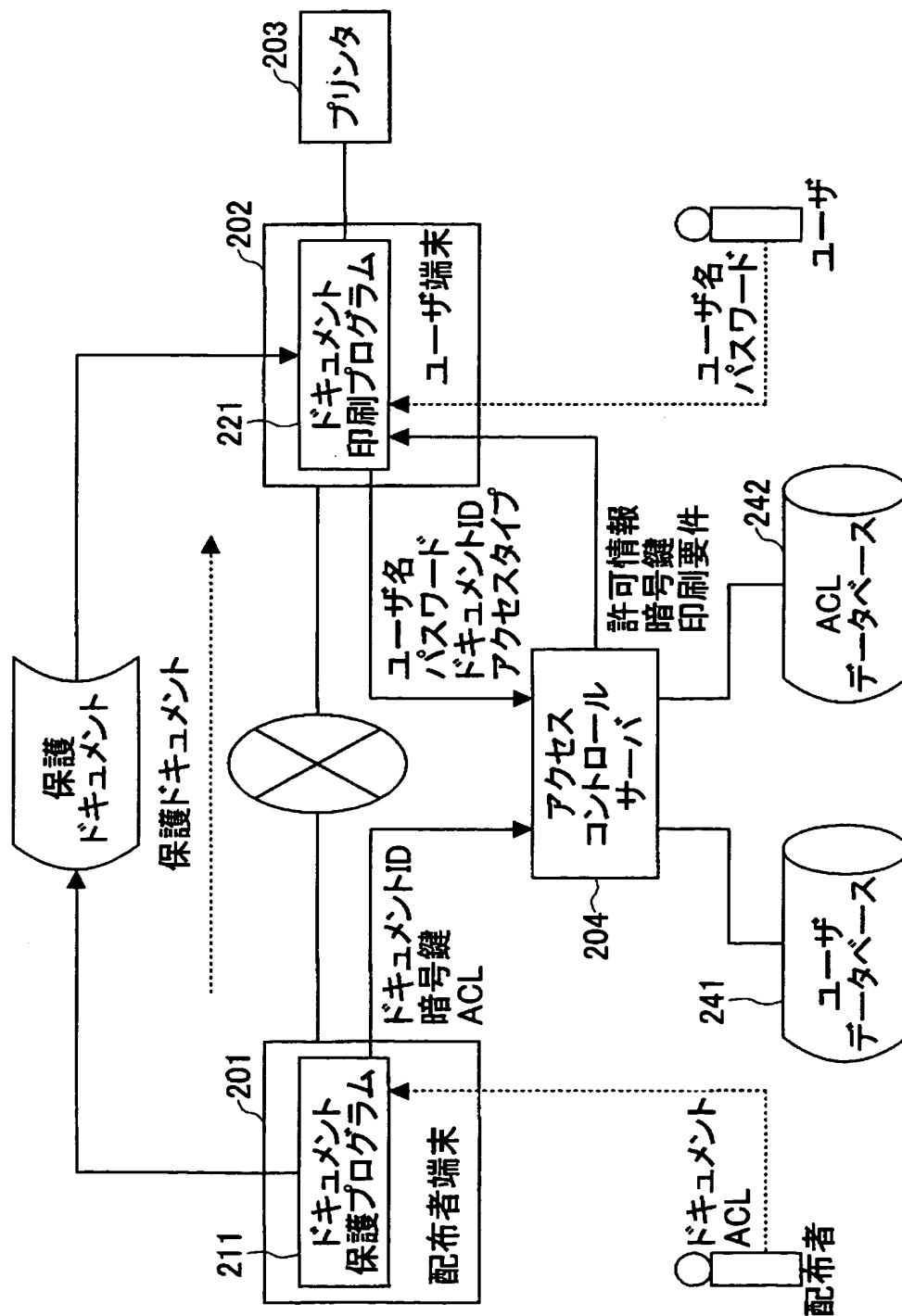
【図 10】

第1の実施形態にかかるドキュメント印刷プログラムの動作を示す図



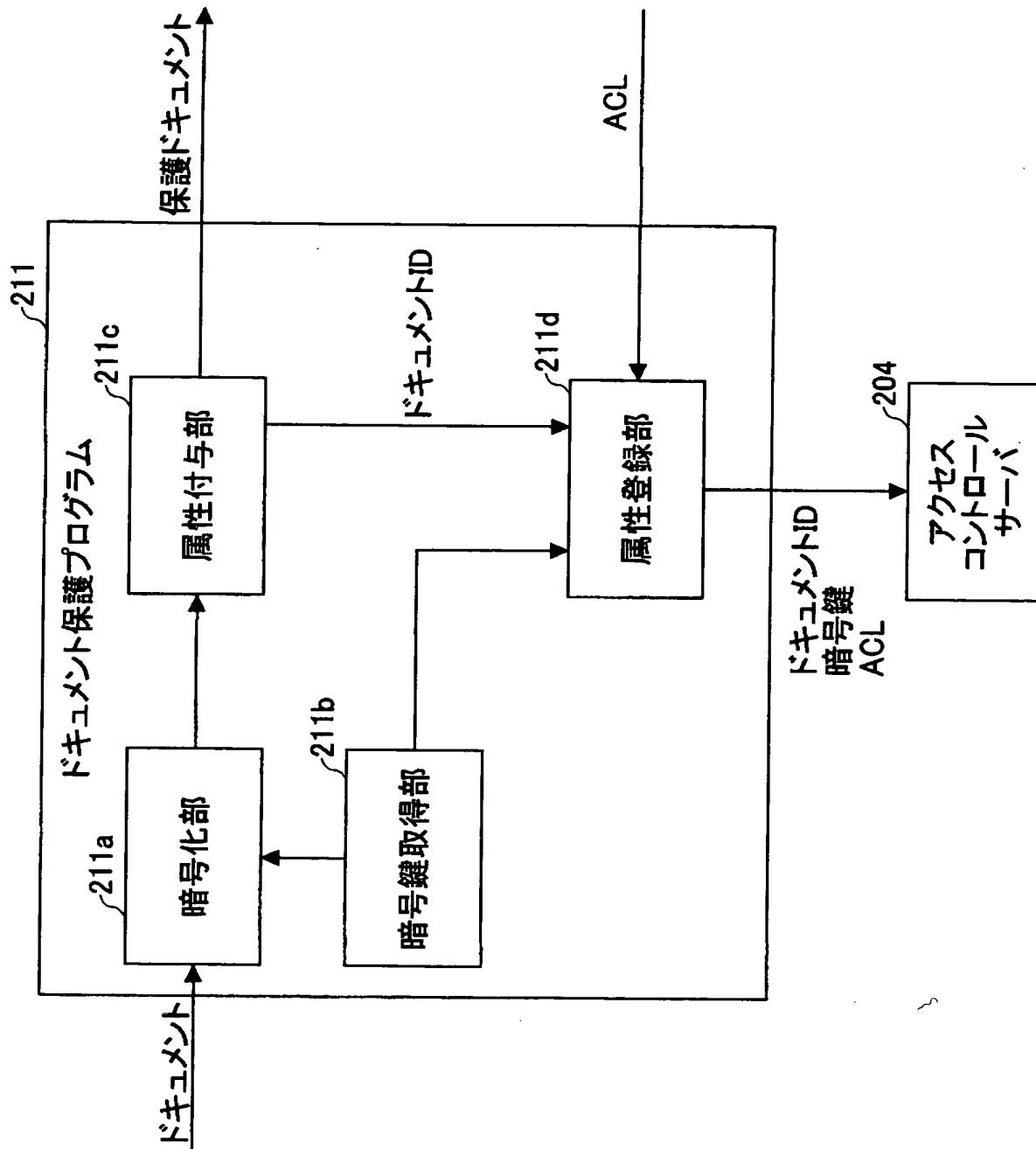
【図 11】

本発明を好適に実施した第2の実施形態にかかる
ドキュメント保護・印刷システムの構成を示す図



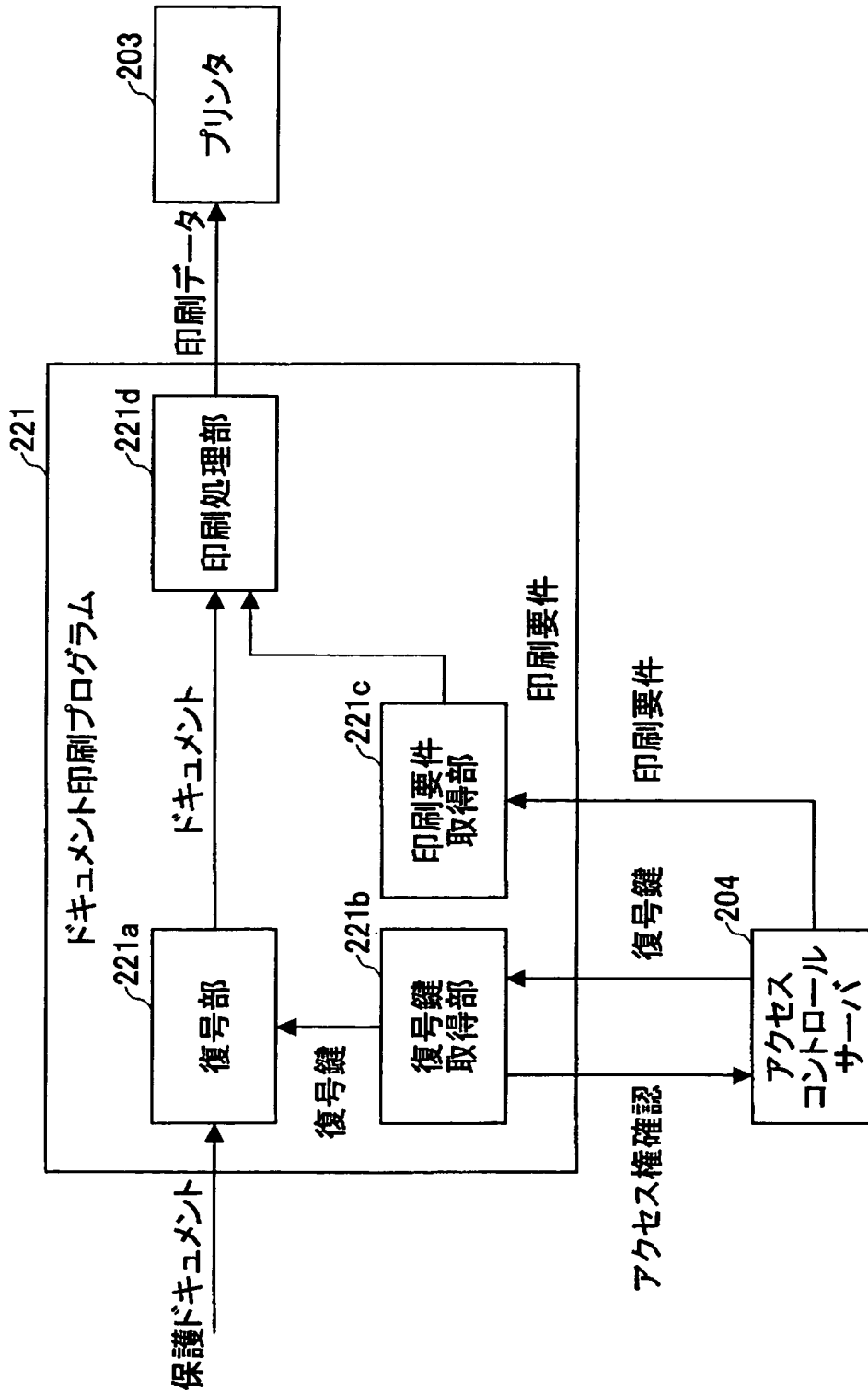
【図 12】

ドキュメント保護プログラムの構成例を示す図



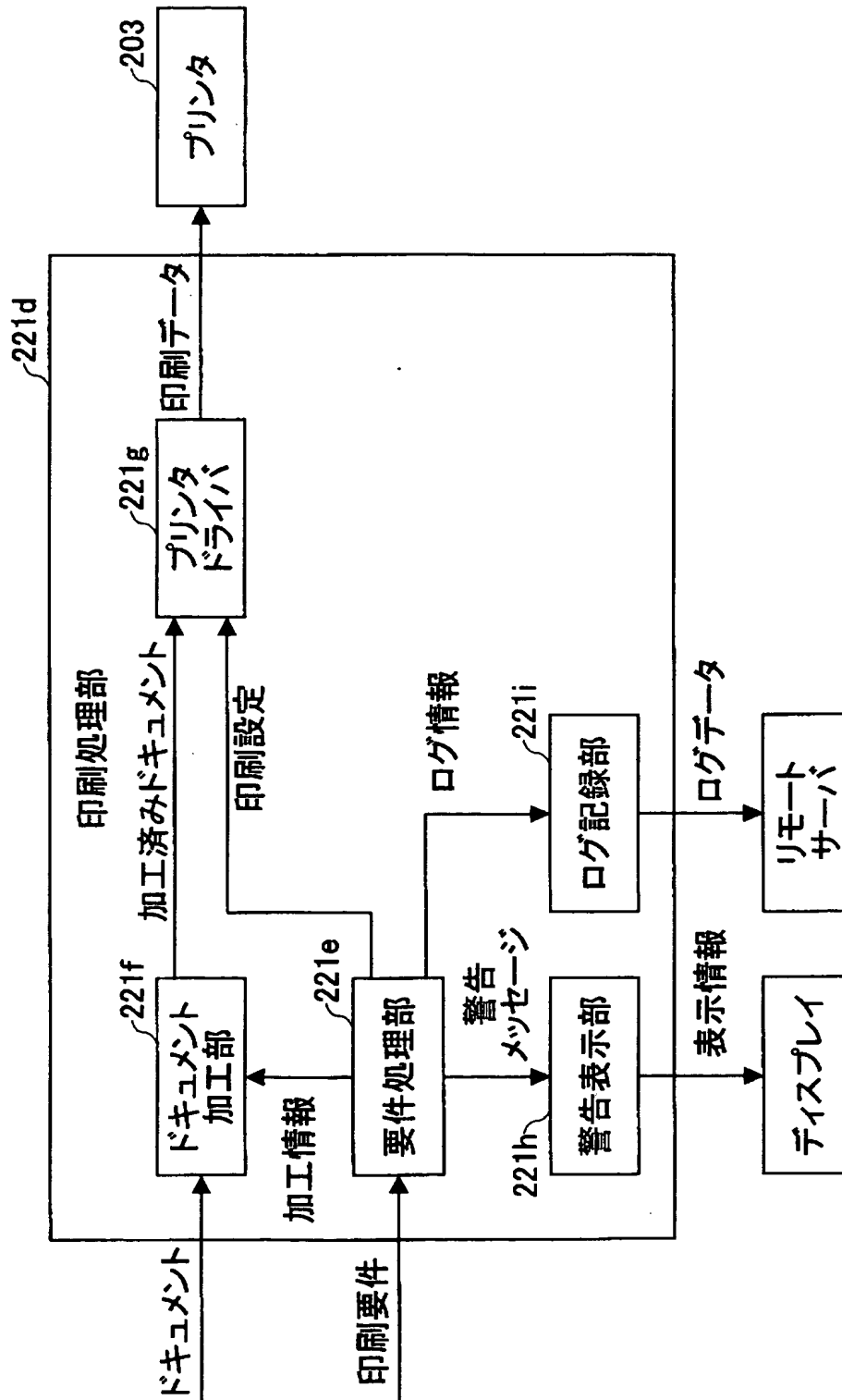
【図 13】

ドキュメント印刷プログラムの構成例を示す図



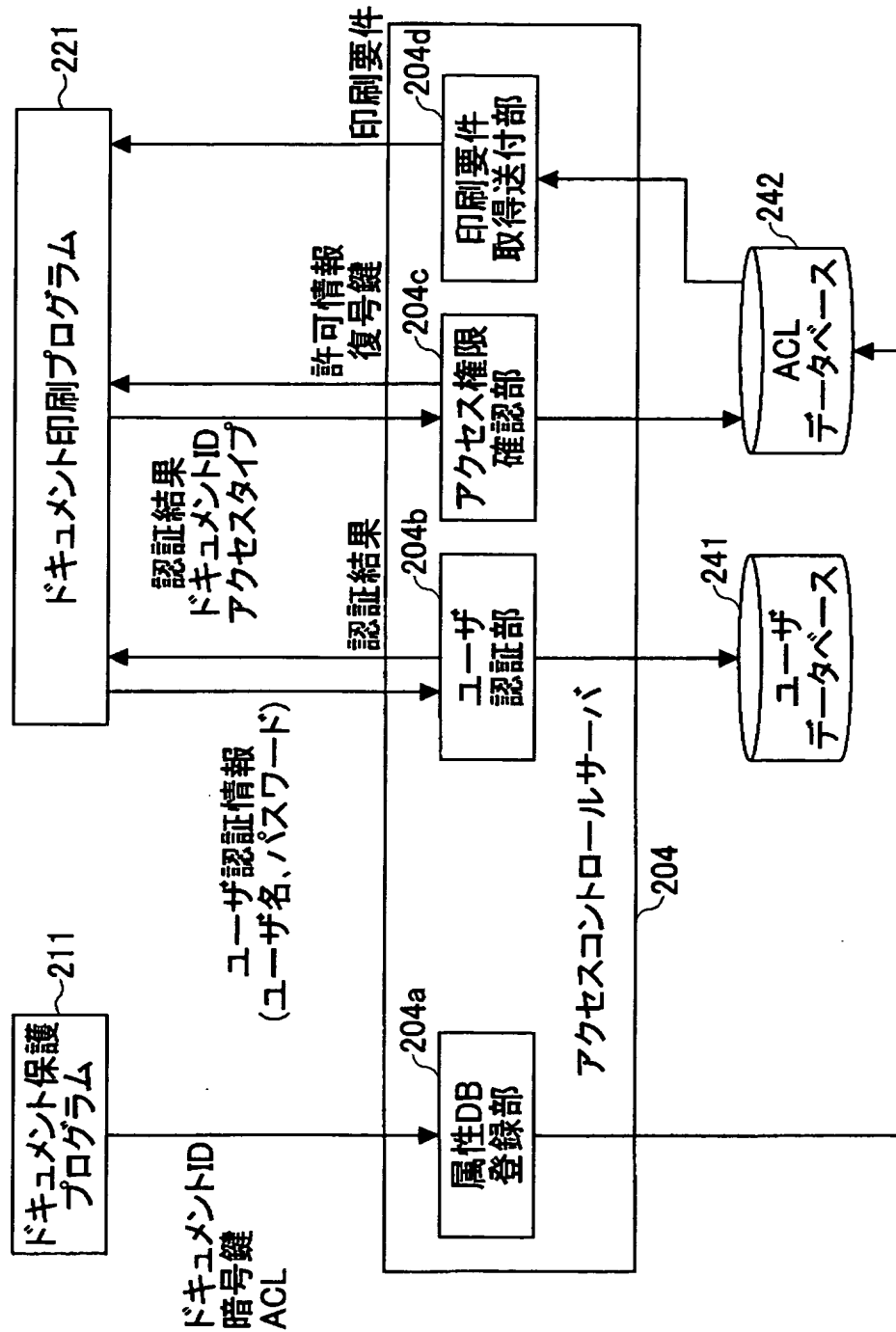
【図 14】

印刷処理部の構成例を示す図



【図 15】

アクセスコントロールサーバの構成例を示す図



【図 16】

ACLの構成例を示す図

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	—
	Write	Denied	—
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	—
	Write	Denied	—
	Print	Denied	—
	Hardcopy	Denied	—
⋮			

【図 17】

ACLデータベースに記録される情報の構造例を示す図

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

【図 18】

ACLの設定を要求する画面の例を示す図

アクセス制御リスト

グループ名またはユーザー名

グループ: Administrators
グループ: 第一設計室メンバー
ユーザー: taro.yamada
ユーザー: hanako.tanaka

taro.yamadaのアクセス許可

	許可	要件
フル コントロール	<input type="checkbox"/>	<input type="checkbox"/>
変更	<input type="checkbox"/>	<input type="checkbox"/>
印刷	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
読み取り	<input checked="" type="checkbox"/>	<input type="checkbox"/>

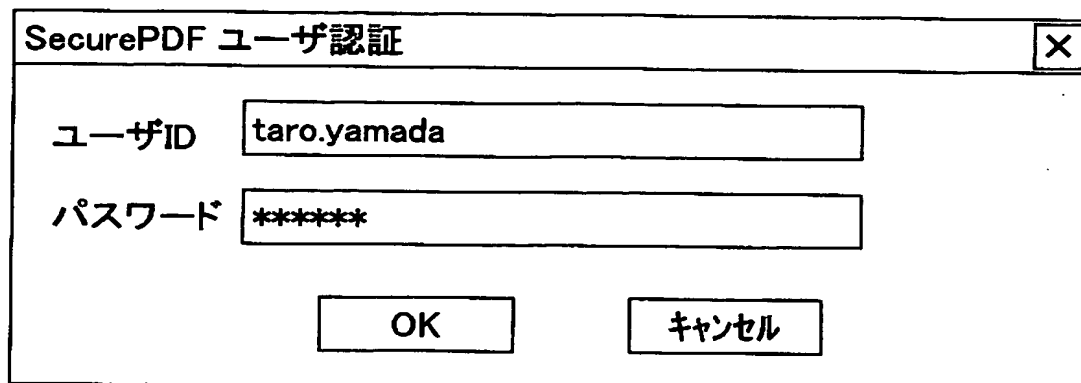
印刷要件 指定 補足情報

機密印刷	<input type="checkbox"/>	
マル秘スタンプ	<input type="checkbox"/>	
ウォーターマーク	<input checked="" type="checkbox"/>	CONFIDENTIAL
地紋印刷	<input type="checkbox"/>	

ファイル:

【図19】

ユーザ名(ユーザID)とパスワードを要求する画面の例を示す図

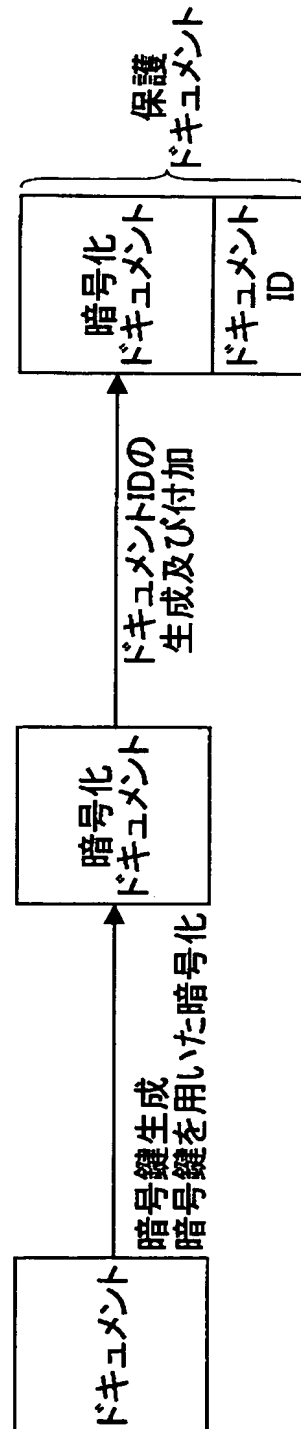


A screenshot of a user authentication dialog box titled "SecurePDF ユーザ認証". The dialog box has a standard Windows-style title bar with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled "ユーザID" and contains the text "taro.yamada". The second field is labeled "パスワード" and contains seven asterisks "*****". Below the input fields, there are two buttons: "OK" on the left and "キャンセル" (Cancel) on the right.

SecurePDF ユーザ認証	
ユーザID	taro.yamada
パスワード	*****
<div>OK キャンセル</div>	

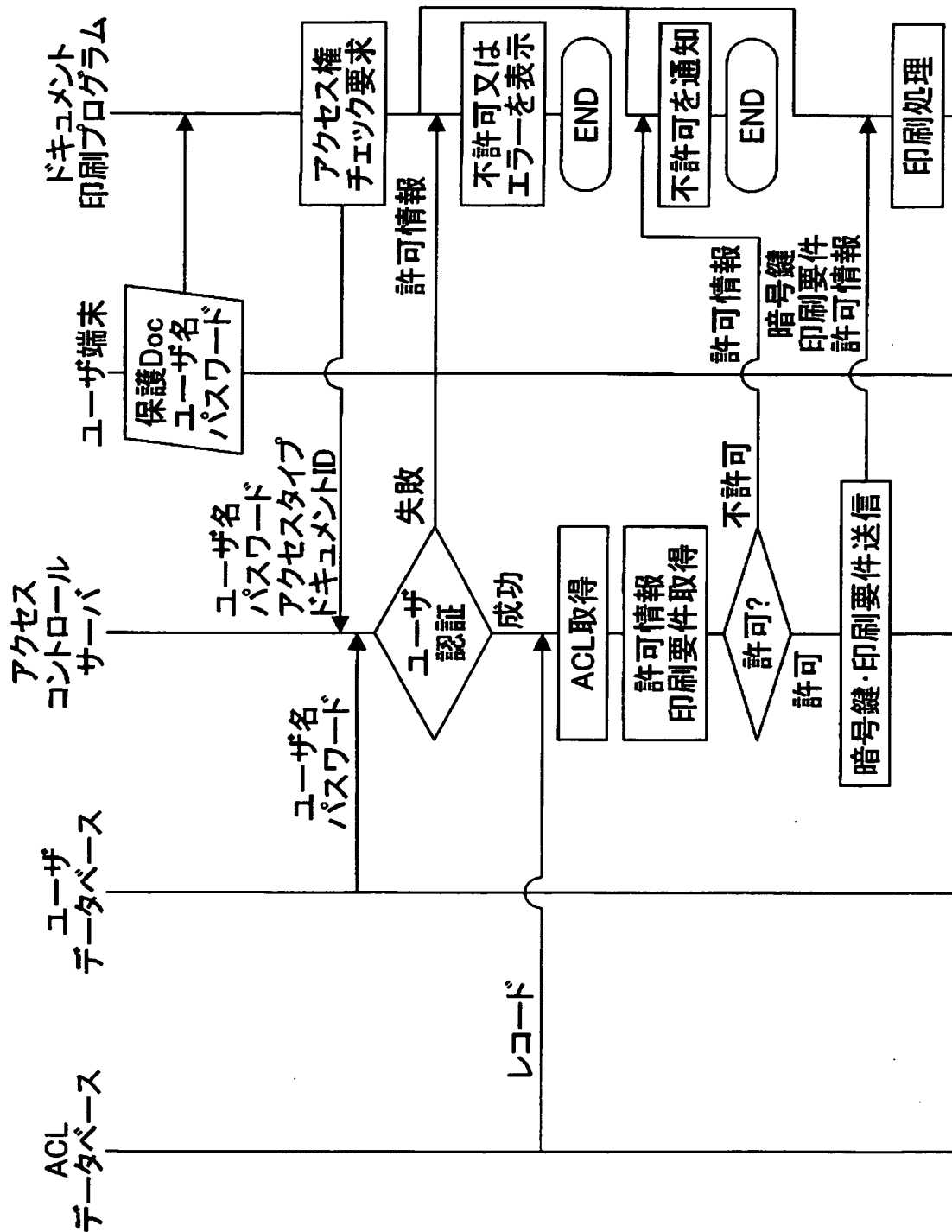
【図 20】

第2の実施形態にかかるドキュメント保護プログラムの動作を示す図



【図 21】

第2の実施形態にかかるドキュメント印刷プログラムおよび
アクセスコントロールサーバの動作の流れを示す図



【図 22】

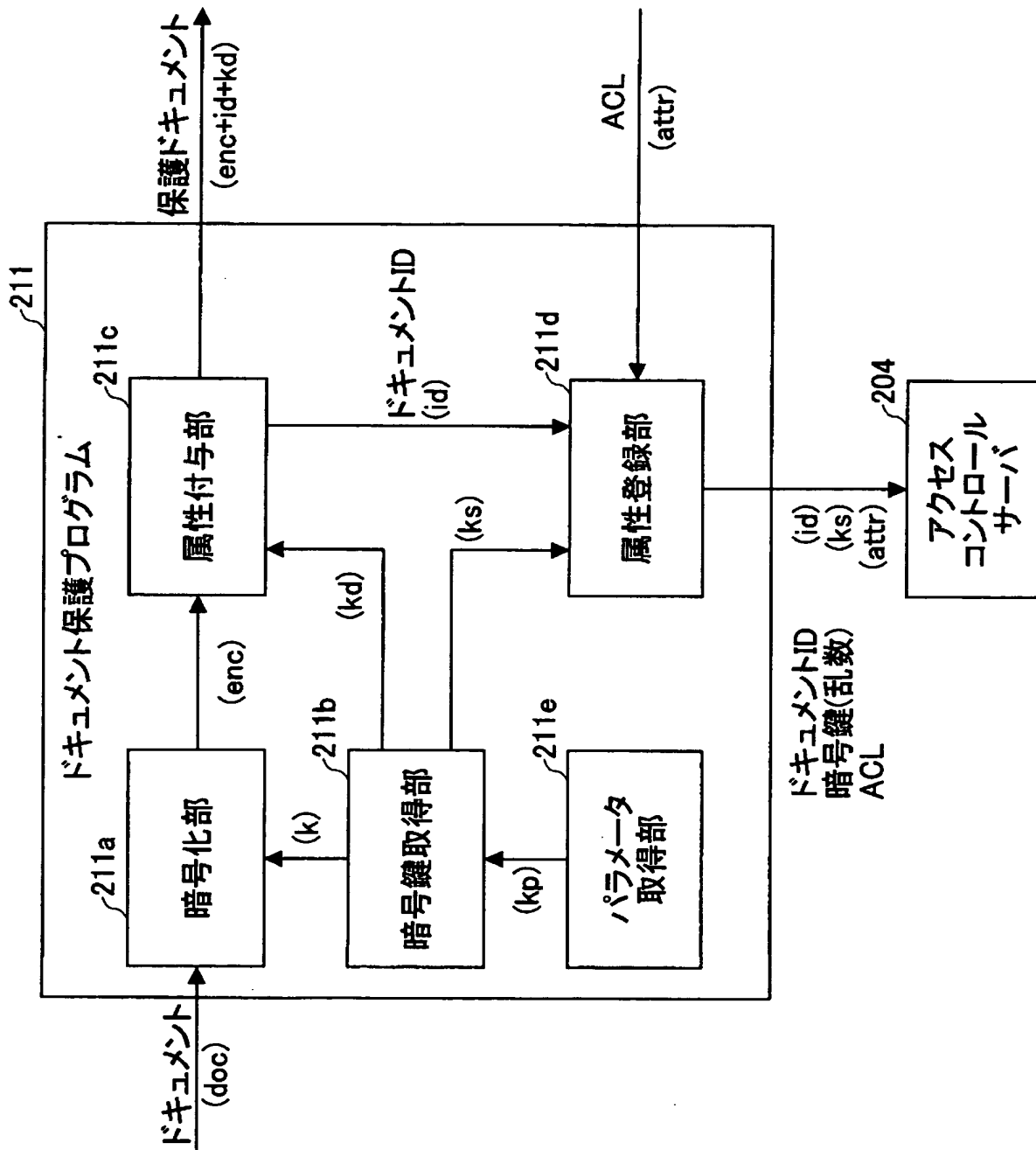
アクセスコントロールサーバへのSOAPによる
問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowed xmlns:m="http://sample.com/sample">
      <sessionId>adfkla;iowoemads</sessionId>
      <userId>taro.yamada</userId>
      <docId>shm000000000003</docId>
      <accessType>print</accessType>
    </m:isAllowed>
  </s:Body>
</s:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
      <isAllowedReturn>
        <allowed xsi:type="xsd:boolean">true</allowed>
        <requirements>
          <item>
            <requirement>private_access</requirement>
          </item>
          <item>
            <requirement>watermark</requirement>
          </item>
          <supplement>CONFIDENTIAL</supplement>
        </requirements>
      </isAllowedReturn>
    </m:isAllowedResponse>
  </s:Body>
</s:Envelope>
```

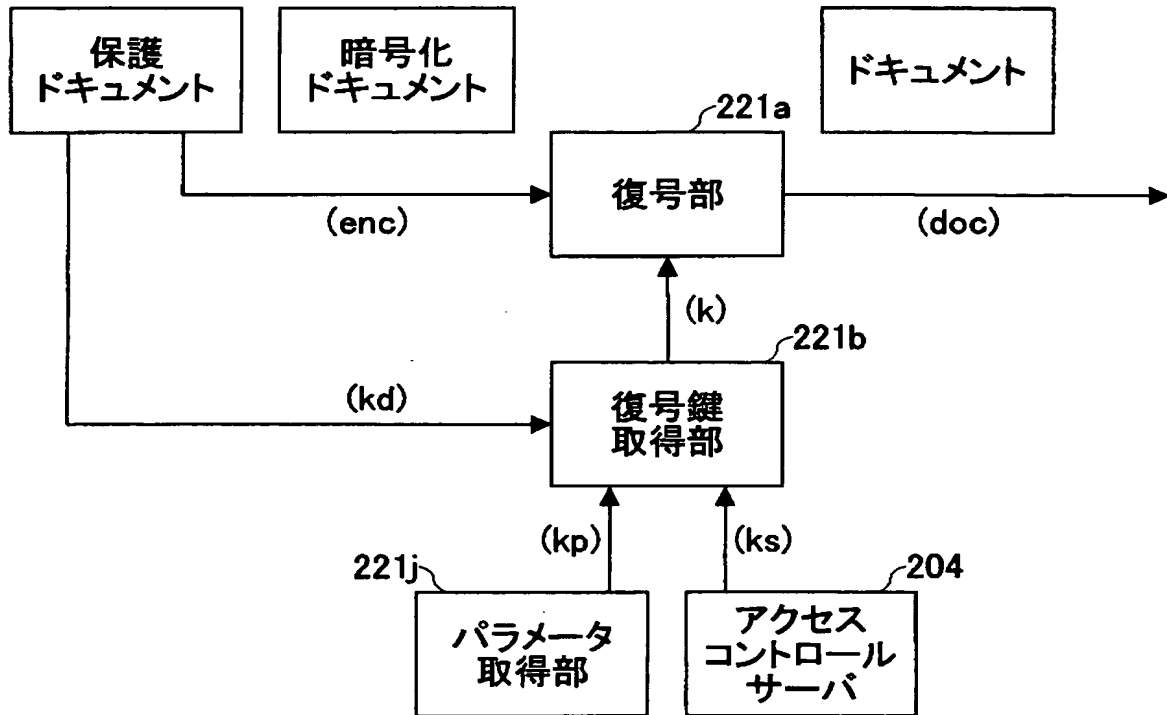
【図 23】

ドキュメント保護プログラムの構成例を示す図



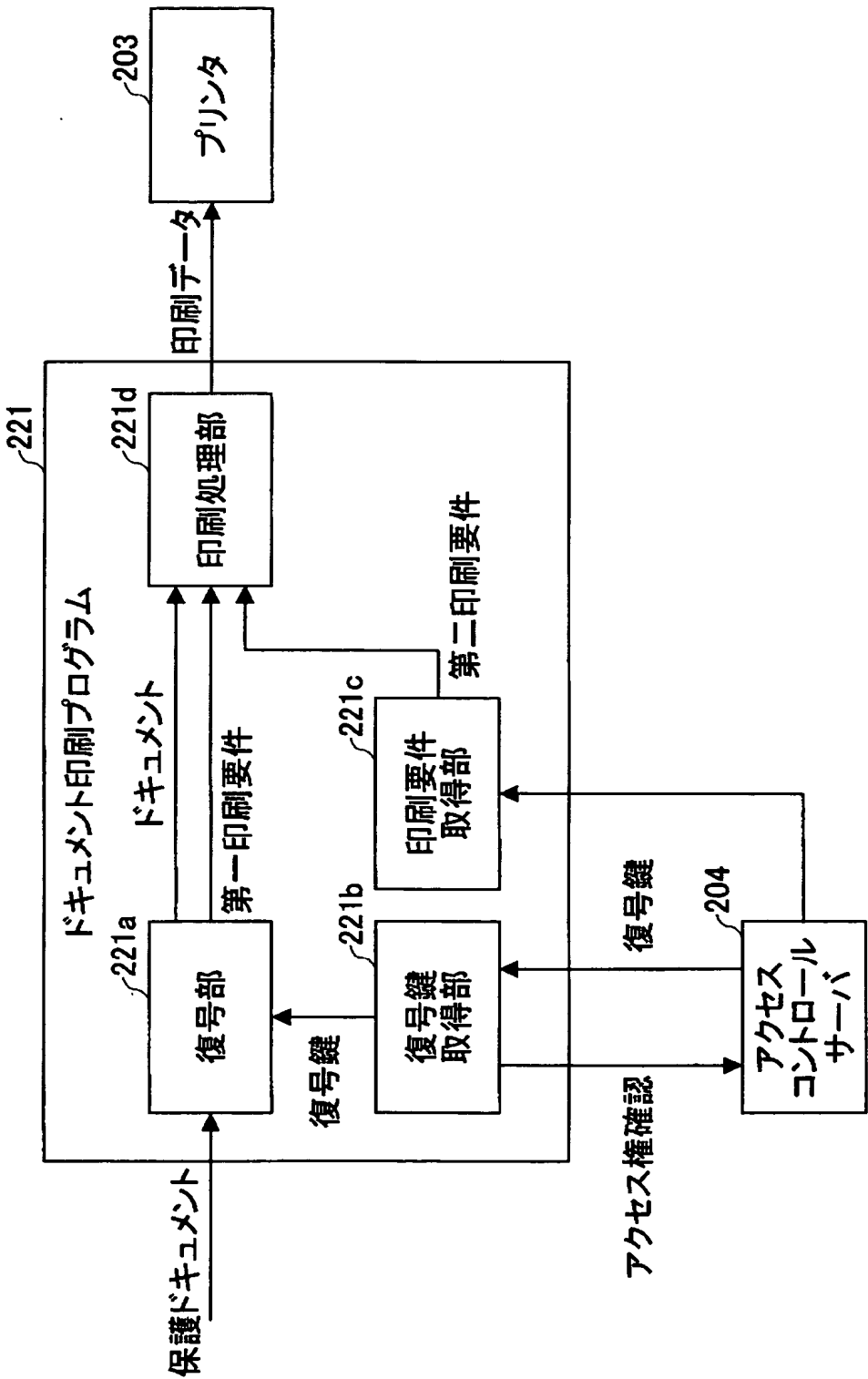
【図 24】

復号の様子を示す図



【図 25】

ドキュメント印刷プログラムの構成例を示す図



【図 2 6】

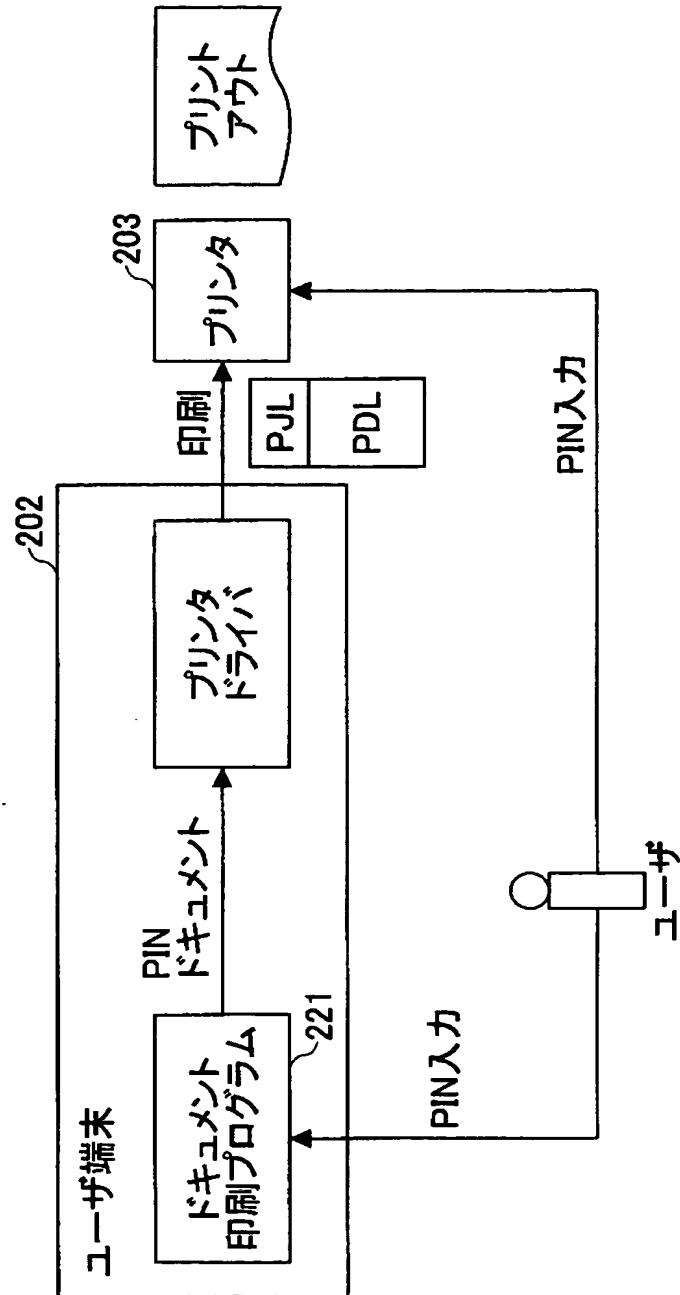
プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバに P I N (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでその P I N を入力しなければプリントアウトされない機能。

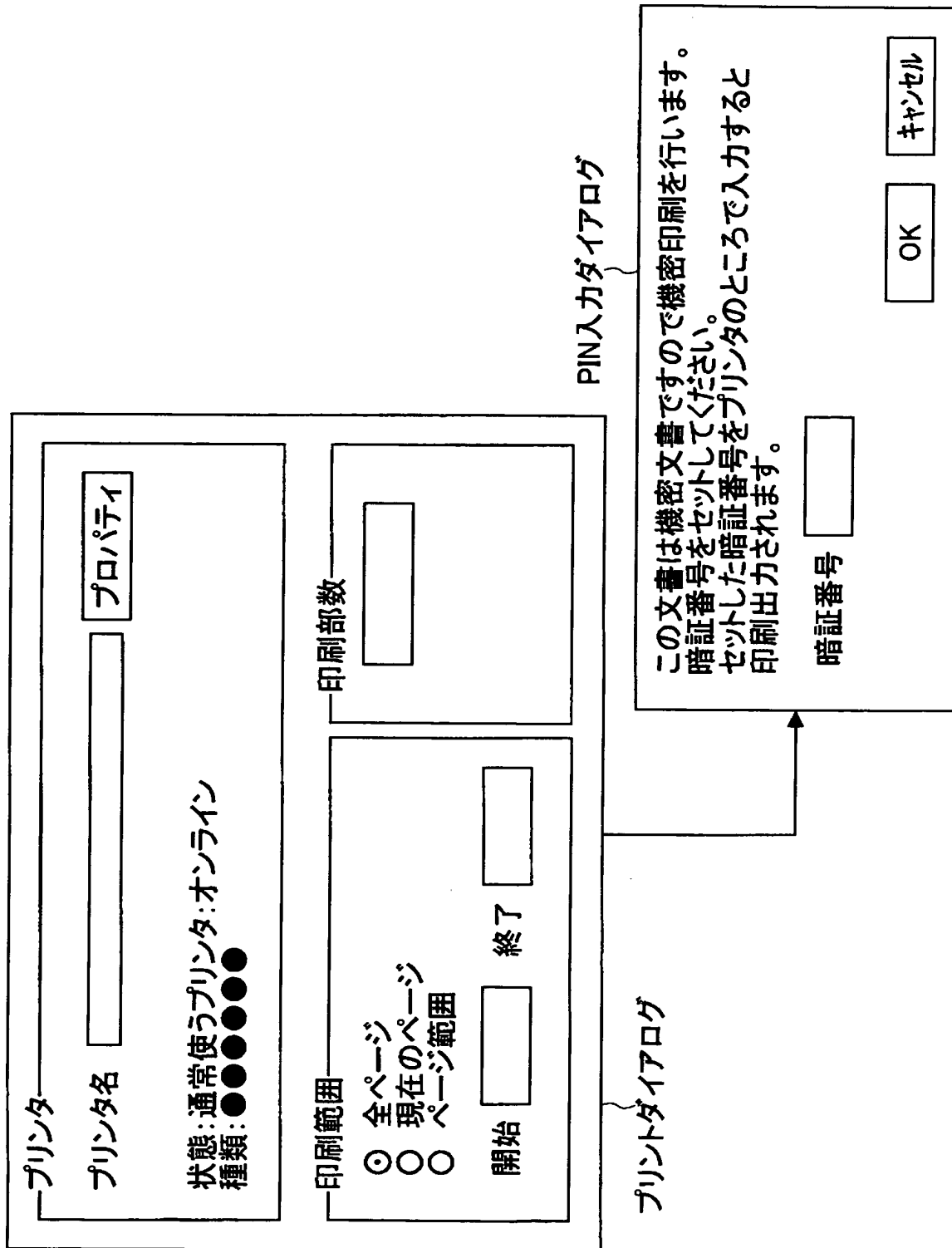
【図 27】

PACが設定されたドキュメントを印刷する際の処理を示す図



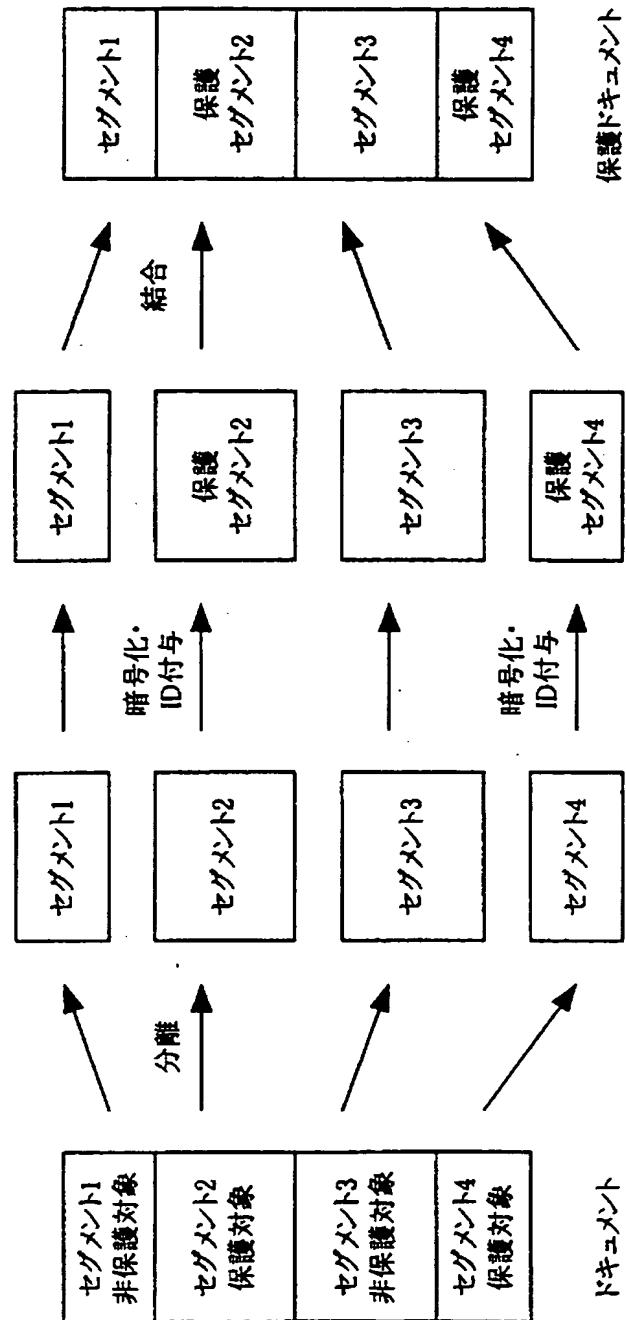
【図 28】

PIN入力のダイアログを示す図



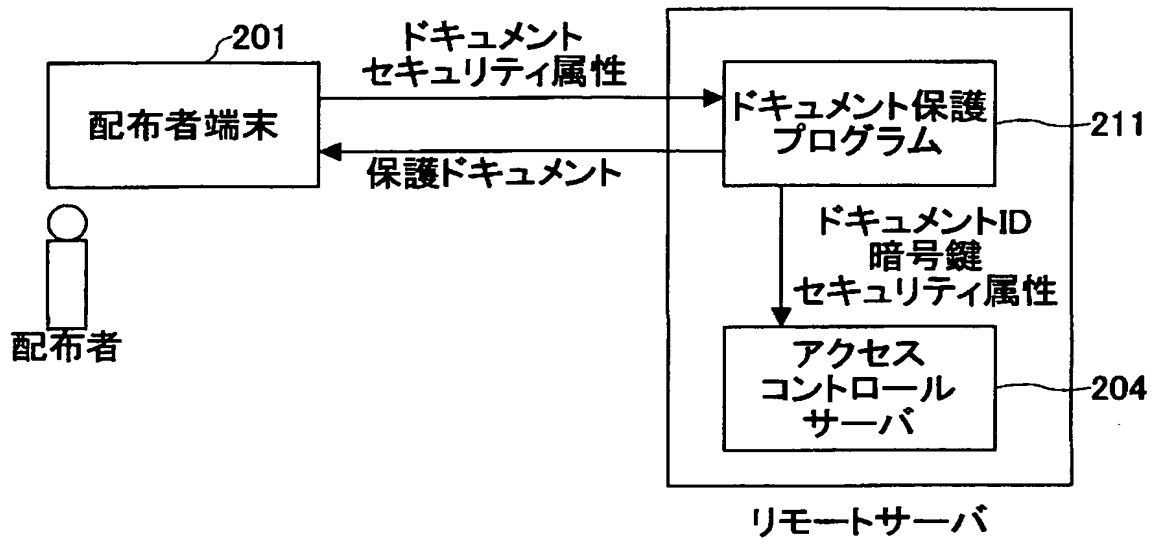
【図 29】

ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図



【図 30】

ドキュメント保護プログラムをリモートサーバ上に
配置した状態を示す図



【書類名】 要約書

【要約】

【課題】 プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。

【解決手段】 ドキュメントファイルに関連付けられている印刷要件を取得する手段と、上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを備えるドキュメント印刷プログラムと、ドキュメントファイルの保護を行うドキュメント保護プログラムとにより構成される。

【選択図】 図 1

特願 2 0 0 3 - 3 1 4 4 6 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー